アクセス制御の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Access Control List（ACL; アクセス制御リスト）を設定する手順について説明します。ACL の設定は、スーパバイザ エンジンに搭載されているハードウェアのタイプによって異なります。詳細については、「ハードウェアの要件」（p.15-3）を参照してください。

（注） この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

（注） Policy-Based ACL（PBACL）設定の詳細については、「PBACL の設定」（p.42-21）を参照してください。

この章で説明する内容は、次のとおりです。

（注） 特に明記されていないかぎり、この章で説明する情報および手順は、Policy Feature Card 3B/3BXL（PFC3B/PFC3BXL; ポリシー フィーチャ カード 3B/3BXL）を搭載した Supervisor Engine 32、PFC3A/PFC3B/PFC3BXL を搭載した Supervisor Engine 720、PFC2 を搭載した Supervisor Engine 2、および PFC を搭載した Supervisor Engine 1 に適用されます。

ACL の機能概要

従来、スイッチが動作するのはレイヤ 2 でのみでした。スイッチが VLAN（仮想 LAN）内のトラフィックをスイッチングし、ルータが VLAN 間のトラフィックをルーティングしていました。Catalyst 6500 シリーズ スイッチは、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）を搭載し、レイヤ 3 スイッチング（Multilayer Switching [MLS; マルチレイヤ スイッチング]）を使用することによって、VLAN 間の高速パケット ルーティングをサポートしています。スイッチがパケットをブリッジングすると、パケットはルータに渡されずに内部的にルーティングされたあと、再びブリッジングされて宛先に送信されます。このプロセスの実行中、スイッチは VLAN 内でブリッジングされるパケットを含み、スイッチングするすべてのパケットをアクセス制御できます。

Cisco IOS ACL が、VLAN 間でルーティングされるトラフィックのアクセス制御を行い、VLAN ACL（VACL）がすべてのパケットのアクセス制御を行います。

パケットの分類には、標準 Cisco IOS ACL および拡張 Cisco IOS ACL を使用します。分類されたパケットには、アクセス制御（セキュリティ）、暗号化、Policy-Based Routing（PBR）など、さまざまな機能が適用されます。標準および拡張 Cisco IOS ACL は、ルータのインターフェイス上だけで設定し、ルーテッド パケットに適用されます。

VACL は、IP および IPX プロトコルのレイヤ 3 アドレスに基づくアクセス制御を行います。サポートされないプロトコルのアクセス制御は、MAC（メディア アクセス制御）アドレス経由で実行されます。VACL は（ブリッジングおよびルーティングされた）すべてのパケットに適用され、任意の VLAN インターフェイス上で設定することができます。VLAN 上で VACL を設定すると、その VLAN に送信されてきた（ルーティングまたはブリッジングされた）すべてのパケットが、VACL チェックの対象になります。パケットは、スイッチ ポートを通じて、またはルーティングされてからルータ ポートを通じて VLAN に送信されます。

（注）Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

ハードウェアの要件

Catalyst 6500 シリーズ スイッチ上で ACL を設定するには、次のハードウェアが必要です。

- Cisco IOS ACL
  - PFC および MSFC または MSFC2 搭載の Supervisor Engine 1
  - PFC2 および MSFC2 搭載の Supervisor Engine 2
  - PFC3A/PFC3B/PFC3BXL および MSFC3 搭載の Supervisor Engine 720
  - PFC3B/PFC3BXL および MSFC2A 搭載の Supervisor Engine 32
- VACL および Quality of Service（QoS; サービス品質）ACL
  - PFC 搭載の Supervisor Engine 1
  - PFC2 搭載の Supervisor Engine 2
  - PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720
  - PFC3B/PFC3BXL 搭載の Supervisor Engine 32

（注）スイッチ上でサポートされる QoS フィーチャ セットは、スーパバイザ エンジン上に搭載されているスイッチング エンジン ドータ カードによって異なります。詳細については、第 49 章「QoS の設定」を参照してください。

サポートされる ACL

ここでは、Catalyst 6500 シリーズ スイッチがサポートしている ACL について説明します。

- QoS ACL（p.15-4）
- Cisco IOS ACL（p.15-4）
- VACL（p.15-5）

QoS ACL

QoS ACL はスイッチ上で設定することができます。第 49 章「QoS の設定」を参照してください。

Cisco IOS ACL

Cisco IOS ACL は、MSFC VLAN インターフェイス上で設定します。ACL は、一連の順序に基づく Access Control Entry（ACE; アクセス制御エントリ）によって、アクセス制御を行います。他の多くの機能もまた、フロー指定のために ACL を使用します。たとえば、（Web Cache Coordination Protocol [WCCP] に基づく）Web キャッシュ リダイレクト機能では、ACL を使用して、Web キャッシュ エンジンにリダイレクトする HTTP フローを指定します。

ほとんどの Cisco IOS 機能は、特定の方向（着信または発信）でインターフェイスに適用されます。ただし、機能によってはグローバルな ACL を使用します。このような機能では、指定した方向のすべてのインターフェイス上に ACL が適用されます。たとえば、TCP 代行受信は、発信方向のすべてのインターフェイス上に適用されるグローバル ACL を使用します。

1 つの Cisco IOS ACL を、特定のインターフェイスの複数の機能と併用できます。また、1 つの機能で複数の ACL を使用することもできます。複数の機能で 1 つの ACL を共有する場合、Cisco IOS ソフトウェアは同じ ACL を何度も検証します。

Cisco IOS ソフトウェアは、特定のインターフェイスおよび方向に設定された各機能について、関連 ACL を検証します。ルータの特定のインターフェイス上にパケットが送信されると、Cisco IOS ソフトウェアは、そのインターフェイス上に設定されているすべての着信機能について、次のような関連 ACL を検証します。

- 着信 ACL（標準、拡張、および再帰、またはそのいずれか）
- 暗号化 ACL（MSFC 上では非サポート）
- ポリシー ルーティング ACL
- 外部から内部へのアドレス変換を指定する Network Address Translation（NAT; ネットワーク アドレス変換）

パケットがルーティングされると、次のホップに転送される前に、Cisco IOS ソフトウェアは出力インターフェイスに設定された発信機能について、次のすべての関連 ACL を検証します。

- 発信 ACL（標準、拡張、および再帰、またはそのいずれか）
- 暗号化 ACL（MSFC 上では非サポート）
- NAT ACL（内部から外部へのアドレス変換）
- WCCP ACL
- TCP 代行受信 ACL

VACL

ここでは、VACL について説明します。

- VACL の概要（p.15-5）
- VACL でサポートされる ACE（p.15-5）
- 分割および非分割トラフィックの処理（p.15-6）

VACL の概要

VACL では、すべてのトラフィックをアクセス制御できます。スイッチ上で VACL を設定し、VLAN が着信または発信するようルーティングされる、または VLAN 内でブリッジングされるすべてのパケットに VACL を適用できます。VACL は、セキュリティ パケット フィルタリングを完全に実行し、トラフィックを特定の物理スイッチ ポートに転送します。Cisco IOS ACL と異なり、VACL には方向（入力または出力）を定義しません。

VACL は、IP および IPX のレイヤ 3 アドレスに基づいて設定します。他のプロトコルはすべて、MAC アドレスおよび MAC VACL を使用する Ethertype によってアクセス制御されます。

注意　IP トラフィックおよび IPX トラフィックは、MAC VACL ではアクセス制御されません。その他のトラフィック タイプ（AppleTalk、DECnet など）はすべて MAC トラフィックとして分類され、MAC VACL によってアクセス制御されます。

（注）　Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）、では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

VACL を適用できるのは、Catalyst 6500 シリーズ スイッチ経由で転送されるパケットだけです。ハブ上のホスト間または Catalyst 6500 シリーズ スイッチに接続している他のスイッチを経由するトラフィックに対して、VACL を適用することはできません。

VACL でサポートされる ACE

VACL には、ACE の順序リストが設定されています。各 VACL に設定できるのは、1 タイプの ACE だけです。各 ACE には、パケットの内容に対応する多数のフィールドがあります。各フィールドに、関連するビットを示す関連ビット マスクを指定します。各 ACE には、条件に一致したパケットをどのように処置するかを指定する 1 つの動作が関連付けられます。この動作は、機能によって異なります。Catalyst 6500 シリーズ スイッチは、ハードウェアで次の 3 タイプの ACE をサポートしています。

- IP ACE
- IPX ACE
- Ethernet ACE

表 15-1 に、各 ACE タイプの関連パラメータを示します。

表 15-1　ACE のタイプおよびパラメータ

ACE タイプ	TCP または UDP[1]	ICMP[1]	その他の IP[1]	IPX	イーサネット[2]
レイヤ 4 パラメータ	送信元ポート				
	送信元ポート演算子				
	宛先ポート				
	宛先ポート演算子	ICMP コード[1]			
	該当なし	ICMP タイプ	該当なし		
レイヤ 3 パラメータ	IP ToS バイト	IP ToS バイト	IP ToS バイト		
	IP 送信元アドレス	IP 送信元アドレス	IP 送信元アドレス	IPX 送信元ネットワーク	
	IP 宛先アドレス	IP 宛先アドレス	IP 宛先アドレス	IPX 宛先ネットワーク	
				IPX 宛先ノード	
	TCP または UDP	ICMP	その他のプロトコル	IPX パケット タイプ	
レイヤ 2 パラメータ					Ethertype
					イーサネット送信元アドレス
					イーサネット宛先アドレス

1. IP ACE
2. IP バージョン 4 または IPX 以外のイーサネット パケット

分割および非分割トラフィックの処理

TCP/UDP または任意のレイヤ 4 プロトコル トラフィックは、分割されると、レイヤ 4 情報（レイヤ 4 送信元 / 宛先ポート）が失われます。この場合、アプリケーションに基づくセキュリティを適用するのは困難です。ただし、分割トラフィックかどうかを識別して、他の TCP/UDP トラフィックと区別することができます。

ACE のレイヤ 4 パラメータは、オフセット 0 のフラグメントを持つ非分割トラフィックおよび分割トラフィックをフィルタリングできます。オフセットが 0 以外の IP フラグメントは、レイヤ 4 ポート情報が失われているので、フィルタリングすることはできません。パケット分割に対応する ACE の例を示します。

次に、1.1.1.1（ポート 68）からのトラフィックが分割されていた場合、最初のフラグメントだけをポート 4/3 に転送する例を示します。ポート 68 からの他のトラフィックはこのエントリの条件とは一致しません。

```
redirect 4/3 tcp host 1.1.1.1 eq 68 host 255.255.255.255
```

次に、1.1.1.1（ポート 68）から発信され、2.2.2.2（ポート 34）を宛先とするトラフィックを許可する例を示します。パケットが分割されている場合、最初のフラグメントはこのエントリの条件と一致するので、許可されます。ただし、オフセットが 0 以外のフラグメントも、デフォルトの分割結果として許可されます。

```
permit tcp host 1.1.1.1 eq 68 host 2.2.2.2 eq 34
```

次に、1.1.1.1（ポート 68）から発信され、2.2.2.2（ポート 34）を宛先とするトラフィックのうち、オフセットが 0 の分割を拒否する例を示します。オフセットが 0 以外のフラグメントは、デフォルトとして許可されます。

```
deny tcp host 1.1.1.1 eq 68 host 2.2.2.2 eq 34
```

Release 6.1(1) より前のソフトウェア リリースでは、フラグメント フィルタリングは完全にトランスペアレントです。**permit tcp .... port eq** *port_number* などの ACE を入力すると、この ACL の先頭に permit tcp any any fragments という ACE がソフトウェアによって暗黙的に付加されます。

Release 6.1(1) 以降のソフトウェア リリースでは、**fragment** オプションが設定されています。**fragment** キーワードを指定しない場合は、旧リリースと同じ結果になります。**fragment** キーワードを指定すると、フラグメントのグローバルな許可ステートメントは自動的には付加されません。このキーワードにより、フラグメントの処理方法を、より詳細に制御できます。

次の例では、サーバ HTTP 接続用として 10.1.1.2 が設定されています。フラグメント ACE を使用しない場合、ACL の先頭に **permit tcp any any fragments** の ACE が自動的に付加されるので、TCP トラフィックのすべてのフラグメントが許可されます。

```
permit tcp any any fragments
```

1. **permit tcp any host 10.1.1.2 eq www**
2. **deny ip any host 10.1.1.2**
3. **permit ip any any**

上の例でエントリ 1 を次のように変更すると、

1. deny tcp any host 10.1.1.2 eq www

permit tcp any any fragments ACE が ACL の先頭に追加されません。エントリが **deny** ステートメントの場合は、次のアクセスリスト エントリが処理されます。

（注）　**deny** ステートメントは、非初期フラグメント対非フラグメント化または初期フラグメントとは別の方法で処理されます。

fragment キーワードを指定すると、グローバルな TCP/UDP フラグメント許可ステートメントは付加されません。少なくとも 1 つの ACE に **fragment** キーワードが指定されていると、指定した特定の IP アドレス（またはサブネット）宛てのフローを許可する ACE が自動的に付加されます。

次の ACL の例では、**deny tcp any host 10.1.1.2 fragment** エントリにより、ホスト 10.1.1.2 上のすべての TCP ポートへの分割トラフィックの転送を拒否しています。また、**permit udp any host 10.1.1.2 eq 69** エントリにより、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ 10.1.1.2 への接続が許可されています。この場合、**permit for all fragments of udp traffic to host 10.1.1.2** の ACE が自動的に付加されます。この ACE が付加されない場合、フラグメントは **deny ip any host 10.1.1.2** エントリによって拒否されます。

1. **deny tcp any host 10.1.1.2 fragment**
2. **permit tcp any host 10.1.1.2 eq www**
3. **permit udp any host 10.1.1.2 eq 69**
4. **permit udp any gt 1023 10.1.1.2 gt 1023**
5. **deny ip any host 10.1.1.2**
6. **permit ip any any**

ホスト 10.1.1.2 への分割 UDP トラフィックを明示的に停止したい場合には、次の例のように、3 番めのエントリの前に **deny udp any host 10.1.1.2 fragment** を入力します。

[...]

3. **deny udp any host 10.1.1.2 fragment**
4. **permit udp any host 10.1.1.2 eq 69**
5. **permit udp any gt 1023 10.1.1.2 gt 1023**

[...]

VLAN 上での Cisco IOS ACL および VACL の適用

ここでは、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットについて、VLAN に Cisco IOS ACL および VACL を適用する方法について説明します。

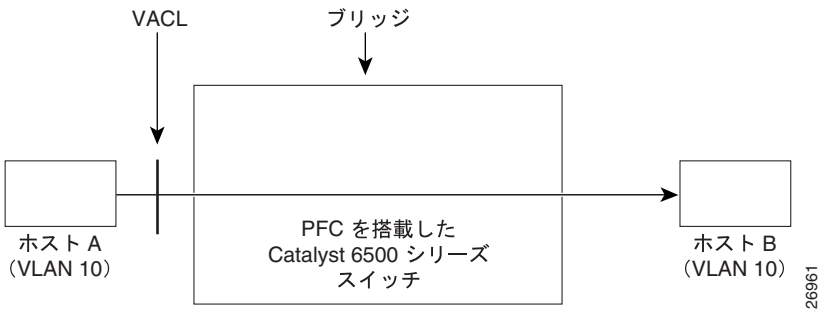
以下、ACL および VACL の適用方法について説明します。

- ブリッジド パケット（p.15-8）
- ルーテッド パケット（p.15-8）
- マルチキャスト パケット（p.15-9）

ブリッジド パケット

図 15-1 は、ブリッジド パケットに ACL がどのように適用されるのかを示しています。ブリッジド パケットの場合は、レイヤ 2 ACL だけが入力 VLAN に適用されます。

図 15-1　ブリッジド パケットへの ACL の適用

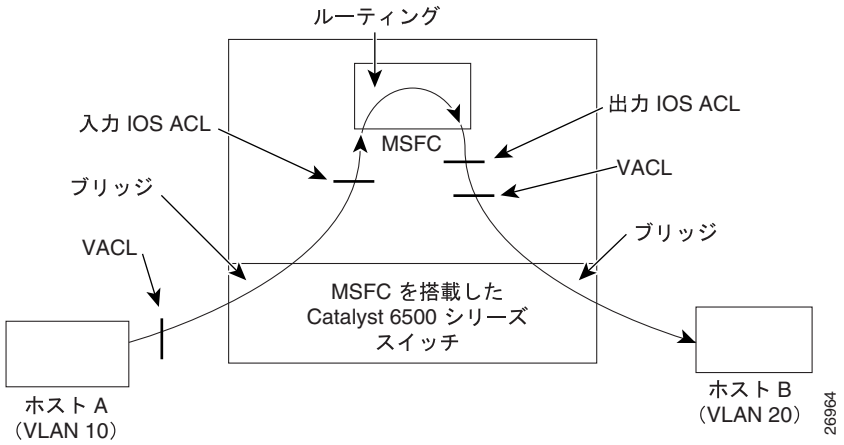


ルーテッド パケット

図 15-2 は、ルーテッド / レイヤ 3 スイッチド パケットに ACL がどのように適用されるのかを示しています。ルーテッド / レイヤ 3 スイッチド パケットの場合、ACL は次の順序で適用されます。

1. 入力 VLAN 用の VACL
2. 入力 Cisco IOS ACL
3. 出力 Cisco IOS ACL
4. 出力 VLAN 用の VACL

図 15-2　ルーテッド パケットへの ACL の適用

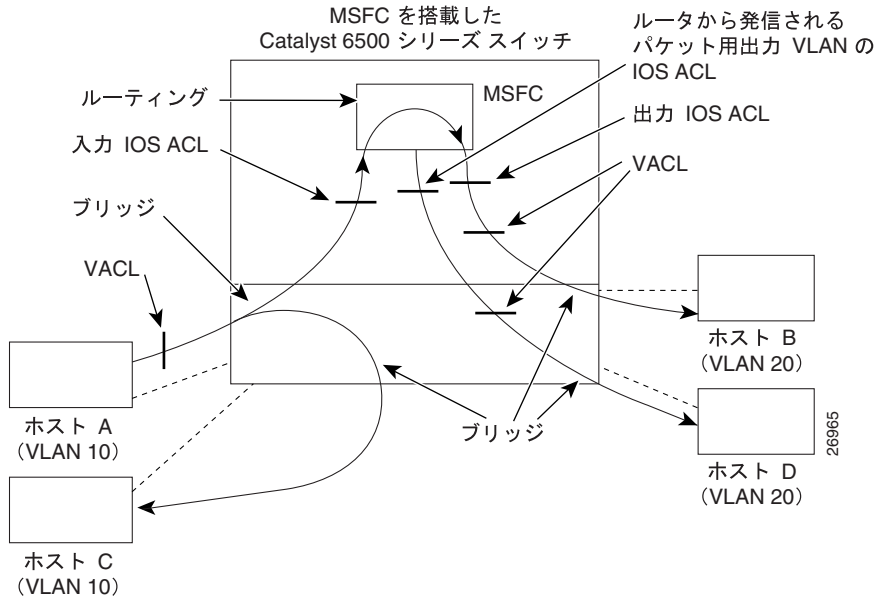


マルチキャスト パケット

図 15-3 は、マルチキャスト拡張を必要とするパケットに対して ACL がどのように適用されるのかを示しています。マルチキャスト拡張を必要とするパケットの場合、ACL は次の順序で適用されます。

1. マルチキャスト拡張を必要とするパケット
   - **a.** 入力 VLAN 用の VACL
   - **b.** 入力 Cisco IOS ACL
2. マルチキャスト拡張後のパケット
   - **a.** 出力 Cisco IOS ACL
   - **b.** 出力 VLAN 用の VACL
3. ルータから発信されたパケット
   - **a.** 出力 VLAN 用の VACL

図 15-3　マルチキャスト パケットへの ACL の適用



ネットワークにおける Cisco IOS ACL の使用方法

（注）Catalyst 6500 シリーズ スイッチのルーテッド VLAN インターフェイス上での Cisco IOS ACL の設定は、他のシスコ製ルータ上での ACL の設定と同じです。Cisco IOS ACL を設定する場合は、「サポートされない機能」（p.15-44）および「VACL 設定時の注意事項」（p.15-45）を参照してください。また、Cisco IOS のコンフィギュレーション ガイドおよびコマンド リファレンスも参照してください。IP の ACL を設定する場合には、『*Network Protocols Configuration Guide*』Part 1 の「Configuring IP Services」を参照してください。

ルータ上にトラフィックを処理する機能（NAT など）を設定すると、その機能に関連付けられている Cisco IOS ACL によって、レイヤ 3 のスイッチングではなくルータにブリッジングされる特定のトラフィックが判別されます。通常、ルータはその機能を適用し、パケットをルーティングします。「PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理」（p.15-11）で、このプロセスの例外をいくつか紹介しています。

（注）冗長 MSFC を搭載したシステムでは、両方の MSFC 上で、Cisco IOS ACL および VACL の同じ ACL 設定を適用する必要があります。

注意　PFC の場合：デフォルトでは、パケットがアクセス グループによって拒否されると、MSFC により Internet Control Message Protocol（ICMP）unreachables（到達不能）メッセージが送信されます。アクセス グループによって拒否されたパケットはハードウェアでは廃棄されず、MSFC が ICMP 到達不能メッセージを生成できるように、MSFC にブリッジングされます。アクセス グループによって拒否されたパケットをハードウェアで廃棄するには、**no ip unreachables** インターフェイス コンフィギュレーション コマンドを使用して、ICMP unreachables をディセーブルにする必要があります。**ip unreachables** コマンドは、デフォルトでイネーブルに設定されています。

PFC2 および PFC3A/PFC3B/PFC3BXL の場合：インターフェイス上で IP unreachables または IP redirect がイネーブルに設定されていると、ハードウェア上で拒否が実行されます。ただし、適切な ICMP 到達不能メッセージを生成するため、少数のパケットが MSFC2/MSFC3 に送信されます。

ここでは、PFC、PFC2、および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる ACL の処理について説明します。

- PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理（p.15-11）
- PFC2 および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理（p.15-13）

PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理

ここでは、PFC でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理について説明します。

（注）　PFC2 および PFC3A/PFC3B/PFC3BXL での Cisco IOS ACL の情報については、「PFC2 および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理」（p.15-13）を参照してください。

ACL 機能の処理では、ソフトウェアによっていくつかのフローを転送する必要があります。ソフトウェア転送フローの割合は、ハードウェア転送フローに比べると、かなり少ないものです。ACL によりロギングが要求されているフローはソフトウェアに渡されますが、ハードウェアによる非ログフローの転送には影響しません。

（注）　**show ip access-list** コマンドの出力に表示されるマッチ カウントは、ハードウェアでアクセス制御されたパケット数ではありません。

（注）　送信元ホストのノード番号を指定した IPX Cisco IOS ACL を、ハードウェアのスイッチ上で実行することはできません。そのため、MSFC がソフトウェアで ACL を処理することになります。この処理は、システムのパフォーマンスを著しく低下させます。

ここでは、各種 ACL とトラフィック フローがハードウェアおよびソフトウェアによってどのように処理されるかについて説明します。

セキュリティ Cisco IOS ACL

PFC では、IP および IPX のセキュリティ Cisco IOS ACL は次のように処理されます。

- セキュリティ ACL の [deny]（拒否）ステートメントと一致するフローは、[ip unreachables]（IP 到達不能）をディセーブルに設定しておくと、ハードウェアによって廃棄されます。[permit]（許可）ステートメントと一致するフローは、ハードウェアによりスイッチングされます。
- セキュリティ アクセス制御用の標準 ACL および拡張 ACL（入力および出力）の許可および拒否動作は、ハードウェアによって処理されます。
- 特定のインターフェイス上の ACL アクセス違反の IP アカウントは、そのインターフェイス上で拒否されたすべてのパケットをソフトウェアに転送することによってサポートされます。この動作は他のフローには影響しません。

- ダイナミック（ロックおよび鍵）ACL フローはハードウェアでサポートされますが、アイドルタイムアウトはサポートされません。
- IPX 標準入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、および宛先ノードの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。ACL に他のパラメータが含まれている場合には、ソフトウェアによって処理されます。
- IPX 拡張入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、宛先ノード、およびプロトコル タイプの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。
- ロギングが必要な ACL フローはソフトウェアによって処理されますが、ハードウェアによる非ログ フローの転送には影響しません。

再帰 ACL

ハードウェアにより、最大 512 の同時再帰セッションがサポートされています。再帰 ACL が適用されている際は、フロー マスクが VLAN-full flow に変更されています。

TCP 代行受信

TCP 代行受信は、DoS 攻撃の一種である TCP SYN フラッディング攻撃から TCP サーバを保護するソフトウェアを実装します。TCP 代行受信は、TCP 接続要求を代行受信して検証することにより、SYN フラッディング攻撃を防止できるようにします。代行受信モードの場合、TCP 代行受信ソフトウェアはクライアントからサーバに送られる、拡張アクセス リストと一致する TCP SYN パケットを代行受信します。ソフトウェアは宛先サーバの代わりにクライアントとの接続を確立します。接続が正常に確立されると、クライアントの代わりにサーバとの接続を確立して、2 つの半接続をトランスペアレントにバインドします。このプロセスにより、到達不能なホストからの接続要求がサーバに到達しないようになります。ソフトウェアは接続されている間、代行受信を継続してパケットを転送します。

ポリシー ルーティング

ポリシー ルーティングが必要なフローは、ソフトウェアによって処理されますが、ハードウェアによる非ポリシー ルーティング フローの転送には影響しません。ルート マップに複数の [match]（一致）コマンドが含まれている場合、すべての一致条件を満たしているパケットだけが、ポリシー ルーティングされます。ただし、ルート マップに [match ip address] および [match length] の両方が含まれている場合には、[match ip address] コマンドの ACL に一致するすべてのトラフィックが、[match length] の条件を満たしているかどうかに関係なく、ソフトウェアに転送されます。ルート マップに match length コマンドだけが含まれている場合は、インターフェイスが受信したすべてのパケットがソフトウェアに転送されます。

mls ip pbr グローバル コマンドを使用してハードウェアのポリシー ルーティングをイネーブルにすると、すべてのポリシー ルーティングがハードウェアで実行されます。

⚠ **注意**　**mls ip pbr** コマンドを使用してポリシー ルーティングをイネーブルにした場合、各インターフェイスにポリシー ルーティングが設定されているかどうかに関係なく、ハードウェアのすべてのインターフェイスにポリシー ルーティングが適用されます。

WCCP

WCCP リダイレクトの対象になる HTTP 要求は、ソフトウェアによって処理されます。サーバおよびキャッシュ エンジンからの HTTP 応答は、ハードウェアで処理されます。

NAT

NAT が必要なフローは、ソフトウェアによって処理されますが、ハードウェアによる非 NAT フローの転送には影響しません。

ユニキャスト RPF チェック

ユニキャスト RPF 機能は、PFC 上のハードウェアでサポートされています。ACL ベースの RPF チェックの場合、ユニキャスト RPF ACL によって拒否されたトラフィックは、RPF 検証のために MSFC に転送されます。

注意　ACL ベースのユニキャスト RPF では、ACL によって拒否されたパケットは、CPU に RPF 検証のために送信されます。DoS 攻撃の場合には、このようなパケットは拒否 ACE にほぼ一致するので、CPU に転送されます。トラフィックが多い状況では、これによって CPU の利用率が高くなります。

（注）　ACL ベースの RPF チェックでは、廃棄抑制統計はサポートされていません。

ブリッジ グループ

Cisco IOS ブリッジ グループ ACL は、ソフトウェアによって処理されます。

PFC2 および PFC3A/PFC3B/PFC3BXL でのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理

ここでは、PFC2 および PFC3A/PFC3B/PFC3BXL で構成されたスイッチでのハードウェアおよびソフトウェアによる Cisco IOS ACL の処理について説明します。

ACL 機能の処理では、いくつかのフローをソフトウェアに転送する必要があります。ソフトウェア転送フローの割合は、ハードウェア転送フローに比べると、かなり少ないものです。ACL によりロギングが要求されているフローはソフトウェアに渡されますが、ハードウェアによる非ログ フローの転送には影響しません。

（注）　**show ip access-list** コマンドの出力に表示されるマッチ カウントは、ハードウェアでアクセス制御されたパケット数ではありません。

（注）　送信元ホストのノード番号を指定した IPX Cisco IOS ACL を、ハードウェアのスイッチ上で実行することはできません。そのため、MSFC がソフトウェアで ACL を処理することになります。この処理は、システムのパフォーマンスを著しく低下させます。

（注）Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

ここでは、各種 Cisco IOS ACL とトラフィック フローが、PFC2 または PFC3A/PFC3B/PFC3BXL で構成されたスイッチで、ハードウェアおよびソフトウェアによってどのように処理されるかについて説明します。

セキュリティ Cisco IOS ACL

PFC2 または PFC3A/PFC3B/PFC3BXL で構成されたスイッチの IP および IPX のセキュリティ Cisco IOS ACL は次のように処理されます。

- [ip unreachables] または [ip redirect] オプションがイネーブルの場合、ACL の [deny] ステートメントと一致するフローのパケットの大半がハードウェアで廃棄されます。少数のパケットだけは、ルータから適切な ICMP 到達不能メッセージを送信するためにソフトウェアに渡されます。
- セキュリティ アクセス制御用の標準 ACL および拡張 ACL（入力および出力）の許可および拒否動作は、ハードウェアによって処理されます。
- 特定のインターフェイス上の ACL アクセス違反の IP アカウントは、そのインターフェイス上で拒否されたすべてのパケットをソフトウェアに転送することによってサポートされています。この動作は他のフローには影響しません。
- ダイナミック（ロックおよび鍵）ACL フローはハードウェアでサポートされていますが、アイドル タイムアウトはサポートされていません。
- IPX 標準入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、および宛先ノードの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。ACL に他のパラメータが含まれている場合には、ソフトウェアによって処理されます。
- IPX 拡張入力 ACL および出力 ACL は、ACL パラメータが IPX 送信元ネットワーク、宛先ネットワーク、宛先ノード、およびプロトコル タイプの場合（またはそのいずれかの場合）、ハードウェアによってサポートされます。
- ロギングが必要な ACL フローはソフトウェアによって処理されますが、ハードウェアによる非ログ フローの転送には影響しません。

Cisco IOS ACL ロギングのレート制限

Cisco IOS ACL ロギングのレート制限によって、ブリッジド ACE の MSFC CPU に送信されるパケット数が制限されます。ログ オプションが指定された Cisco IOS ACL の結果が拒否または許可の場合、ACE がブリッジングされます。このブリッジ動作の結果、Cisco IOS ACL ロギングは MSFC CPU の過負荷をもたらします。Cisco IOS ACL ロギングのレート制限を設定すると、ブリッジングされた ACE はレート制限付きで MSFC にリダイレクトされます。

Cisco IOS ACL ロギングのレート制限設定時の注意事項

ここでは、Cisco IOS ACL ロギングのレート制限設定時の注意事項について説明します。

- **set acllog ratelimit** *rate* コマンドまたは **clear acllog** コマンドを入力したあとで、MSFC をリセットするか、**log** キーワードが適用された ACE を備えた MSFC インターフェイスに対して shutdown/no shutdown を実行する必要があります。

  set acllog ratelimit *rate* コマンドを入力すると、リセットまたは shutdown/no shutown 動作によってブリッジングされた ACE はレート制限付きで MSFC にリダイレクトされます。

  clear acllog コマンドを入力すると、リセットまたは shutdown/no shutdown 動作によってスイッチは元の動作に戻り、ブリッジ動作は元のままです。

- **set acllog ratelimit** *rate* コマンドを入力して指定する *rate* には、1 ～ 1000 の値を使用できます。*rate* は、リダイレクト ACE と一致し、MSFC に送信される 1 秒当たりのパケット数です。実際の 1 秒当たりのパケット数が指定した *rate* より大きい場合は、指定した *rate* を超えるパケットは廃棄されます。*rate* には、500 パケット / 秒を指定することを推奨します。

Cisco IOS ACL ロギングのレート制限の設定

Cisco IOS ACL ロギングのレート制限を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ACL ロギングをイネーブルにして、Cisco IOS ACL ロギング レート制限のレートを指定します。	**set acllog ratelimit** *rate*
ステップ 2	ACL ロギング ステータスを表示します。	**show acllog**

次に、ACL ロギングをイネーブルにして、Cisco IOS ACL ロギング レート制限のレートを 500 に指定する例を示します。

```
Console> (enable) set acllog ratelimit 500
If the ACLs-LOG were already applied, the rate limit mechanism will be effective on
system restart, or after shut/no shut the interface.
Console> (enable)

Console> (enable) show acllog
ACL log rate limit enabled, rate = 500 pps.
Console> (enable)
```

次に、ACL ロギングを消去する（ディセーブルにする）例を示します。ACL ロギングを消去すると、ブリッジ動作は元どおりになり、システムの動作は **set acllog ratelimit** コマンドを発行する前と同じになります。

```
Console> (enable) clear acllog
ACL log rate limit is cleared.
If the ACLs-LOG were already applied, the rate limit mechanism will be disabled on
system restart, or after shut/no shut the interface.
Console> (enable)
```

再帰 ACL

ICMP パケットは、ソフトウェアによって処理されます。TCP/UDP フローの場合は、フローが確立されれば、ハードウェアによって処理されます。再帰 ACL が適用されている際は、フロー マスクが VLAN-full flow に変更されています。

TCP 代行受信

（注）　TCP 代行受信は、Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）または Supervisor Engine 32（PFC3B/PFC3BXL）ではサポートされません。

TCP 代行受信は、DoS 攻撃の一種である TCP SYN フラッディング攻撃から TCP サーバを保護するソフトウェアを実装します。TCP 代行受信は、TCP 接続要求を代行受信して検証することにより、SYN フラッディング攻撃を防止できるようにします。代行受信モードの場合、TCP 代行受信ソフトウェアはクライアントからサーバに送られる、拡張アクセス リストと一致する TCP SYN パケットを代行受信します。ソフトウェアは宛先サーバの代わりにクライアントとの接続を確立します。接続が正常に確立されると、クライアントの代わりにサーバとの接続を確立して、2 つの半接続をトランスペアレントにバインドします。このプロセスにより、到達不能なホストからの接続要求がサーバに到達しないようになります。ソフトウェアは接続されている間、代行受信を継続してパケットを転送します。

PFC2 では、TCP 代行受信が次のようにハードウェアによってサポートされています。

1. TCP 代行受信が設定されている場合、TCP 代行受信 ACL 内の permit ステートメントを含む ACE と一致し、かつセキュリティ ACL によって許可されているすべての TCP SYN パケットは、TCP 代行受信機能を適用するソフトウェアに送信されます。このプロセスは、セキュリティ ACL に SYN フラグが指定されていない場合でも発生します。
2. 接続が正常に確立されると、次の処理が適用されます。
   a. TCP 代行受信で使用されている代行受信モードにタイムアウトが指定されている場合は、所定の接続 / フローに属するすべてのトラフィックがソフトウェアで処理されます。
   b. TCP 代行受信がそれ以外のモードを使用している場合、接続が正常に確立されると、ソフトウェアはハードウェア ショートカットをインストールして、残りのフローをハードウェアでスイッチングします。
3. 接続が正常に確立されない場合は、他のトラフィックはそのフローに属することができません。

ポリシー ルーティング

ポリシー ルーティングが必要なフローは、ルート マップに応じて、ハードウェアまたはソフトウェアによって処理されます。ルート マップに match ip address だけが設定され、set コマンドにネクスト ホップが含まれている場合、そのネクスト ホップが到達可能であれば、パケットはハードウェアに転送されます。ルート マップに複数の match コマンドが含まれている場合、すべての一致条件を満たしているパケットだけが、ポリシー ルーティングされます。ただし、ルート マップに match ip address および match length の両方が含まれている場合には、match ip address コマンドの ACL に一致するすべてのトラフィックが、match length の条件を満たしているかどうかに関係なく、ソフトウェアに転送されます。ルート マップに match length コマンドだけが含まれている場合は、インターフェイスが受信したすべてのパケットがソフトウェアに転送されます。

（注）　PFC2 または PFC3A/PFC3B/PFC3BXL 上では、**mls ip pbr** コマンドは不要です（サポートされていません）。

WCCP

（注）　Release 8.1(x) ～ 8.4(x) では、WCCP は Supervisor Engine 720 または Supervisor Engine 32 でサポートされません。

WCCP リダイレクトの対象になる HTTP 要求は、ソフトウェアによって処理されます。サーバおよびキャッシュ エンジンからの HTTP 応答は、ハードウェアで処理されます。

NAT

NAT が必要なフローは、ソフトウェアによって処理されますが、ハードウェアによる非 NAT フローの転送には影響しません。

ユニキャスト RPF チェック

ユニキャスト RPF は、PFC2 および PFC3A/PFC3B/PFC3BXL 上でハードウェアによってサポートされます。ACL ベースの RPF チェックの場合、ユニキャスト RPF ACL によって拒否されたトラフィックは、RPF 検証のために MSFC2 または MSFC3 に転送されます。

注意　ACL ベースのユニキャスト RPF では、ACL によって拒否されたパケットは、CPU に RPF 検証のために送信されます。DoS 攻撃の場合には、このようなパケットは拒否 ACE にほぼ一致するので、CPU に転送されます。トラフィックが多い状況では、これによって CPU の利用率が高くなります。

（注）　ACL ベースの RPF チェックでは、廃棄抑制統計はサポートされていません。

ブリッジ グループ

Cisco IOS ブリッジ グループ ACL は、ソフトウェアによって処理されます。

VACL と Cisco IOS ACL の併用

ブリッジド トラフィックおよびルーテッド トラフィックの両方をアクセス制御するには、VACL だけを使用するか、Cisco IOS ACL と VACL を組み合わせて使用します。Cisco IOS ACL は、入力用および出力用の両方のルーテッド VLAN インターフェイスに定義することができます。VACL は、ブリッジド トラフィックのアクセスを制御するために定義します。

ACL の VACL deny または redirect ステートメントの条件に一致したフローは、Cisco IOS ACL の設定に関係なく、拒否またはリダイレクトされます。Cisco IOS ACL を VACL と組み合わせて使用する場合は、次の事項に注意してください。

- 発信 ACL に設定したロギングを必要とするパケットは、VACL によって拒否された場合、ロギングされません。
- NAT — VACL は、NAT 変換前のパケットに適用されます。また、変換後のフローをアクセス制御する必要がない場合でも、VACL の設定によっては、変換後のフローがアクセス制御されることがあります。

（注）VACL では、リストの最後に暗黙の拒否ステートメントが付加されます。どの VACL ACE にも一致しないパケットは拒否されます。

ここでは、Cisco IOS ACL の設定、VACL の設定、およびレイヤ 4 演算の注意事項について説明します。

- 同一 VLAN インターフェイス上に Cisco IOS ACL および VACL を設定する場合の注意事項（p.15-18）
- レイヤ 4 演算設定時の注意事項（p.15-25）

同一 VLAN インターフェイス上に Cisco IOS ACL および VACL を設定する場合の注意事項

ここでは、同じ VLAN 上に Cisco IOS ACL *および*VACL の両方を設定する場合の注意事項について説明します。Cisco IOS ACL と VACL を異なる VLAN 上にマッピングする設定では、これらの注意事項は当てはまりません。

Catalyst 6500 シリーズ スイッチのハードウェアは、各方向（入力および出力）についてセキュリティ ACL を 1 度だけ検索します。同じ VLAN 上に Cisco IOS ACL および VACL の両方を適用する場合には、これらをマージする必要があります。Cisco IOS ACL と VACL をマージすると、ACE の数が著しく増加することがあります。

同一 VLAN 上で Cisco IOS ACL と VACL を設定する場合には、Cisco IOS ACL および VACL の両方を、次の注意事項に基づいて設定してください。

（注）**show security acl resource-usage** コマンドを入力すると、使用済みの ACL ストレージの割合が表示されます。

ここでは、Cisco IOS ACL と VACL を設定する場合の注意事項、およびその例を示します。

- 暗黙の拒否ステートメント（p.15-19）
- 動作のグループ化（p.15-19）

- 動作数の制限（p.15-19）
- レイヤ 4 ポート情報の回避（p.15-19）
- Release 7.1(1) より前のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定（p.15-20）
- Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定（p.15-23）

暗黙の拒否ステートメント

できるだけ、ACL の最後に付加される暗黙の拒否ステートメント（deny any any）を使用し、許可するトラフィックだけを ACE に定義してください。すべての拒否エントリを定義して、最後に許可ステートメント（**permit ip any any**）を指定しても、同じ結果になります（例 1 [p.15-21] を参照）。

動作のグループ化

ACL に複数の動作（許可、拒否、リダイレクト）を定義する場合には、各動作をタイプ別にグループ化します。例 3（p.15-22）は、各タイプをグループ化しなかった場合の例を示しています。この例では、6 行めの deny ステートメントが、permit ステートメントと同じグループに入っています。この deny ステートメントを削除すると、合成後のエントリ数を 329 から 53 に減らすことができます。

動作数の制限

許可 ACE のみで構成される ACL は、許可と拒否という 2 つの動作を含んでいます（リストの最後の暗黙の拒否のため）。許可とリダイレクトが設定されている ACL では、許可、リダイレクト、拒否という 3 つの動作を含んでいます（リストの最後の暗黙の拒否のため）。

ACL の設定時に 2 種類の動作だけを指定すると、最良のマージ結果が得られます（許可と拒否、リダイレクトと許可、リダイレクトと拒否のマージ）。

（注）Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースでは、ACL マージのアルゴリズムが改善されているので、ACL の設定時に動作数を制限する必要はありません。

リダイレクトおよび拒否の ACL を定義するには、許可 ACE を使用しません。リダイレクトおよび許可の ACL を定義するには、許可 ACE およびリダイレクト ACE だけを定義し、最後に **permit ip any any** ステートメントを指定します。**permit ip any any** を指定すると、リストの最後に付加される暗黙の拒否（deny ip any）が無効になります（例 4 [p.15-22] を参照）。

レイヤ 4 ポート情報の回避

マージ プロセスが複雑になるので、ACL にはレイヤ 4 情報を入れないでください。full flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）ではなく、IP アドレス（送信元および宛先）だけに基づいてフィルタリングする ACL を定義すると、最良のマージ結果が得られます。

full flow を指定する必要がある場合には、「暗黙の拒否ステートメント」（p.15-19）および「動作のグループ化」（p.15-19）を参照してください。ACL に、IP およびレイヤ 4 情報を含む TCP/UDP/ICMP ACE を指定しなければならない場合には、IP アドレスに基づくトラフィック フィルタリングを優先させ、レイヤ 4 の ACE はリストの最後に指定してください。

Release 7.1(1) より前のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定

（注）　Release 7.1(1) より前のスーパバイザ エンジン ソフトウェア リリースと、7.1(1) 以降のリリースで、マージ結果を比較する場合は、「Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定」（p.15-23）を参照してください。

上記の注意事項に基づいて ACL を設定した場合、ACL のマージ結果をおおまかに推測することができます。

たとえば、ACL A、ACL B、および ACL C があるとします。ACL C を、ACL A と ACL B のマージ結果とした場合、ACL A と ACL B のサイズがわかっていれば、ACL C の上限サイズを次の公式によって概算することができます。ただし、ACL A と ACL B にレイヤ 4 ポート情報が含まれていないことが前提です。

ACL C のサイズ =（ACL A のサイズ）×（ACL B のサイズ）×（2）

（注）　Release 7.1(1) より前のソフトウェア リリースでは、この公式を目安として使用できますが、エントリ数は予想範囲を大幅に上回ることがあります。Release 7.1(1) 以降のソフトウェアリリースでは、新しい ACL マージ アルゴリズムを使用するので、この公式で正確な値を知ることができます。レイヤ 4 ポート情報が含まれている場合は、新しいアルゴリズムでも上限サイズはさらに大きくなります。詳細については、「レイヤ 4 演算設定時の注意事項」（p.15-25）を参照してください。

ACL マージ アルゴリズムには、Binary Decision Diagram（BDD）と Order-Dependent Merge（ODM）の 2 種類があります。ODM は、Release 7.1(1) のソフトウェア リリースで採用された拡張アルゴリズムです。BDD アルゴリズムは、Release 7.1(1) より前のソフトウェア リリースで使用されていました。設定の詳細については、「ACL マージ アルゴリズムの指定」（p.15-47）を参照してください。

（注）　Release 8.1(1) 以降のソフトウェア リリースでは、BDD アルゴリズムはどのプラットフォーム（PFC、PFC2、または PFC3A/PFC3B/PFC3BXL）上でもサポートされなくなりました。デフォルトの ACL マージ アルゴリズムは ODM です。Release 8.1(1) 以降のソフトウェア リリースでは、コマンドが次のように変更されています。**set aclmerge algo** および **set aclmerge bdd** コマンドは削除されました。**show aclmerge** {**bdd** | **algo**} コマンドは **show aclmerge algo** になりました。

ここでは、さまざまな Cisco IOS ACL および VACL 設定によるマージ結果の例を示します。それぞれ 1 つずつの VACL および Cisco IOS ACL を同じ VLAN に設定します。

例 1

次に、VACL の設定が推奨事項に従っていない（ACL の最後に暗黙の拒否動作を指定する代わりに、9 行めに拒否動作を定義）ため、マージの結果、ACE 数が増える例を示します。

```
******** VACL  ***********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  deny tcp any host 194.72.6.51 eq ftp
10 permit tcp any host 194.72.6.51 eq ftp-data
11 permit tcp any host 194.72.6.51
12 permit tcp any eq domain host 194.72.6.51
13 permit tcp any host 194.72.6.51 gt 1023
14 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE **********
has 91 entries entries
```

例 2

例 1 の場合、推奨事項に従って 9 行めを削除し（代わりに、ACL の最後で暗黙の拒否を使用）、9 行めで廃棄するはずだったトラフィックが許可されないように、11 行めおよび 12 行めを変更すると、次のような ACL になり、マージ結果が改善されます。

```
******** VACL **********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  permit tcp any host 194.72.6.51 eq ftp-data
10 permit tcp any host 194.72.6.51 neq ftp
11 permit tcp any eq domain host 194.72.6.51 neq ftp
12 permit tcp any host 194.72.6.51 gt 1023
13 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE ***********
has 78 entries
```

例 3

次に、VACL の設定が推奨事項に従っていない（すべての動作タイプがひとまとめにされていない）ため、マージの結果、ACE 数が著しく増える例を示します。

```
******** VACL  ***********
1  deny ip 0.0.0.0 255.255.255.0 any
2  deny ip 0.0.0.255 255.255.255.0 any
3  deny ip any 0.0.0.0 255.255.255.0
4  permit ip any host 239.255.255.255
5  permit ip any host 255.255.255.255
6  deny ip any 0.0.0.255 255.255.255.0
7  permit tcp any range 0 65534 any range 0 65534
8  permit udp any range 0 65534 any range 0 65534
9  permit icmp any any
10 permit ip any any
******** Cisco IOS ACL **********
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE **********
has 329 entries
```

例 4

次に、VACL の設定が推奨事項に従っていない（3 種類の動作が指定されている）ため、マージの結果、ACE 数が著しく増える例を示します。

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 deny tcp any any lt 30
4 deny udp any any lt 30
5 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********
has 142 entries
```

例 5

次に、例 4 の VACL を変更し、2 種類の動作だけを指定したことによって、マージ結果が大幅に改善される例を示します。

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********
has 4 entries
```

Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定

Release 7.1(1) より前のスーパバイザ エンジン ソフトウェア リリースの場合と同様、7.1(1) 以降のリリースでも次の公式が成り立ちます。ACL C のサイズ ＝（ACL A のサイズ）×（ACL B のサイズ）×（2）。

（注）Release 7.1(1) より前のソフトウェア リリースでは、この公式を目安として使用できますが、エントリ数は予想範囲を大幅に上回ることがあります。Release 7.1(1) 以降のソフトウェアリリースでは、新しい ACL マージ アルゴリズムを使用するので、この公式で正確な値を知ることができます。レイヤ 4 ポート情報が含まれている場合は、新しいアルゴリズムでも上限サイズはさらに大きくなります。詳細については、「レイヤ 4 演算設定時の注意事項」（p.15-25）を参照してください。

ACL マージ アルゴリズムには、BDD と ODM の 2 種類があります。ODM は、Release 7.1(1) で採用された拡張アルゴリズムです。BDD アルゴリズムは、Release 7.1(1) より前のソフトウェア リリースで使用されていました。ソフトウェア設定の詳細については、「ACL マージ アルゴリズムの指定」（p.15-47）を参照してください。

（注）Release 8.1(1) 以降のソフトウェア リリースでは、BDD アルゴリズムはどのプラットフォーム（PFC、PFC2、または PFC3A/PFC3B/PFC3BXL）上でもサポートされなくなりました。デフォルトの ACL マージ アルゴリズムは ODM です。Release 8.1(1) 以降のソフトウェア リリースでは、コマンドが次のように変更されています。**set aclmerge algo** および **set aclmerge bdd** コマンドは削除されました。**show aclmerge {bdd | algo}** コマンドは **show aclmerge algo** になりました。

例

ここでは、さまざまな Cisco IOS ACL および VACL 設定によるマージ結果の例を示します。それぞれ 1 つずつの VACL および Cisco IOS ACL を同じ VLAN に設定します。

例 1

```
******** VACL  ***********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  deny tcp any host 194.72.6.51 eq ftp
10 permit tcp any host 194.72.6.51 eq ftp-data
11 permit tcp any host 194.72.6.51
12 permit tcp any eq domain host 194.72.6.51
13 permit tcp any host 194.72.6.51 gt 1023
14 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********
Using the new algorithm - 17 entries
Using the old algorighm - 91 entries
```

例 2

```
******** VACL  **********
1  permit udp host 194.72.72.33 194.72.6.160 0.0.0.15
2  permit udp host 147.150.213.94 194.72.6.64 0.0.0.15 eq bootps
3  permit udp 194.73.74.0 0.0.0.255 host 194.72.6.205 eq syslog
4  permit udp host 167.221.23.1 host 194.72.6.198 eq tacacs
5  permit udp 194.72.136.1 0.0.3.128 194.72.6.64 0.0.0.15 eq tftp
6  permit udp host 193.6.65.17 host 194.72.6.205 gt 1023
7  permit tcp any host 194.72.6.52
8  permit tcp any host 194.72.6.52 eq 113
9  permit tcp any host 194.72.6.51 eq ftp-data
10 permit tcp any host 194.72.6.51 neq ftp
11 permit tcp any eq domain host 194.72.6.51 neq ftp
12 permit tcp any host 194.72.6.51 gt 1023
13 permit ip  any host 1.1.1.1
******** Cisco IOS ACL ************
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE ***********
Using the new algorithm - 16 entries
Using the old algorithm - 78 entries
```

例 3

```
******** VACL  ***********
1  deny ip 0.0.0.0 255.255.255.0 any
2  deny ip 0.0.0.255 255.255.255.0 any
3  deny ip any 0.0.0.0 255.255.255.0
4  permit ip any host 239.255.255.255
5  permit ip any host 255.255.255.255
6  deny ip any 0.0.0.255 255.255.255.0
7  permit tcp any range 0 65534 any range 0 65534
8  permit udp any range 0 65534 any range 0 65534
9  permit icmp any any
10 permit ip any any
******** Cisco IOS ACL **********
1  deny ip any host 239.255.255.255
2  permit ip any any
******** MERGE **********
Using the new algorithm - 12 entries
Using the old algorithm - 303 entries
```

例 4

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 deny tcp any any lt 30
4 deny udp any any lt 30
5 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********

Using the new algorithm - 6 entries
Using the old algorithm - 142 entries
```

例 5

```
******** VACL  ***********
1 redirect 4/25 tcp host 192.168.1.67 host 255.255.255.255
2 redirect 4/25 udp host 192.168.1.67 host 255.255.255.255
3 permit ip any any
*******  Cisco IOS ACL ***********
1  deny ip any host 239.255.255.255
2  permit ip any any
*******  MERGE **********

Using the new algorithm - 4 entries
Using the old algorithm - 4 entries
```

レイヤ 4 演算設定時の注意事項

ここでは、レイヤ 4 ポート演算使用時の注意事項について説明します。

- レイヤ 4 演算の使用方法（p.15-25）
- LOU の使用（p.15-26）

レイヤ 4 演算の使用方法

スイッチ ハードウェアには、次のタイプの演算子を指定することができます。

- gt（geater than：より大きい）
- lt（less than：より小さい）
- neq（not equal：等しくない）
- eq（equal：等しい）
- range（inclusive range：包含範囲）

1 つの ACL に指定する演算は、9 つまでにしてください。この数を超えると、新しい演算によって影響される ACE が、複数の ACE に分割されることがあります。

（注）　同じ VLAN インターフェイス上に Cisco IOS ACL および VACL の両方を設定する場合も、レイヤ 4 演算の数は合計で 9 以下にすることを推奨します。

レイヤ 4 演算を定義するときは、次の 2 つの注意事項に従ってください。

1. レイヤ 4 演算は、演算子またはオペランドが異なっていると、異なる演算であるとみなされます。次の ACL には 4 つの異なるレイヤ 4 演算が定義されています（[gt 10] と [gt 11] は 2 つの異なるレイヤ 4 演算です）。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
... neq 6 redirect
```

（注）　[eq] 演算子の使用に制限はありません。[eq] 演算子は Logical Operator Unit（LOU）または レイヤ 4 演算ビットを使用しないためです。LOU については、「LOU の使用」（p.15-26）を参照してください。

2. レイヤ 4 演算は、同じ演算子とオペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算になります。次の ACL では、1 つの ACE には送信元ポート、もう 1 つの ACE には宛先ポートが指定されているので、2 つの異なるレイヤ 4 演算が定義されていることになります。

```
... Src gt 10 ...
... Dst gt 10
```

（注）　ACL のレイヤ 4 ポート演算リソースの使用状況を調べるには、**show security acl resource-usage** コマンドを使用します。

LOU の使用

LOU は、演算子とオペランドの組み合わせを保存するレジスタです。すべての ACL は LOU を使用します。最大 32 の LOU があります。各 LOU には、2 つの異なる演算子 / オペランドの組み合わせを保存できますが、range 演算子だけは例外です。レイヤ 4 演算は、次のように LOU を使用します。

- gt は、1/2 LOU を使用します。
- lt は、1/2 LOU を使用します。
- neq は、1/2 LOU を使用します。
- range は、1 LOU を使用します。
- eq は、LOU を使用しません。

たとえば、次の ACL では、1 つの LOU に 2 つの異なる演算子とオペランドが保存されます。

```
... Src gt 10 ...
... Dst gt 10
```

以下は、より詳細な例です。

```
ACL1
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 redirect
... (src port) neq 6 redirect
... (dst port) gt 10 deny

ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 permit
... (dst port) neq 6 redirect
```

レイヤ 4 演算数と LOU の使用数は、次のとおりです。

- ACL1 のレイヤ 4 演算：5
- ACL2 のレイヤ 4 演算：4
- LOU：4

LOU は、次のように使用されています。

- LOU 1 に、[gt 10] および [lt 9] が保存されます。
- LOU 2 に、[gt 11] および [neq 6] が保存されます。
- LOU 3 に、[gt 20] が保存されます（半分は空き）。
- LOU 4 に、[range 11 13] が保存されます（range は 1 LOU を使用）。

ネットワークでの VACL の使用

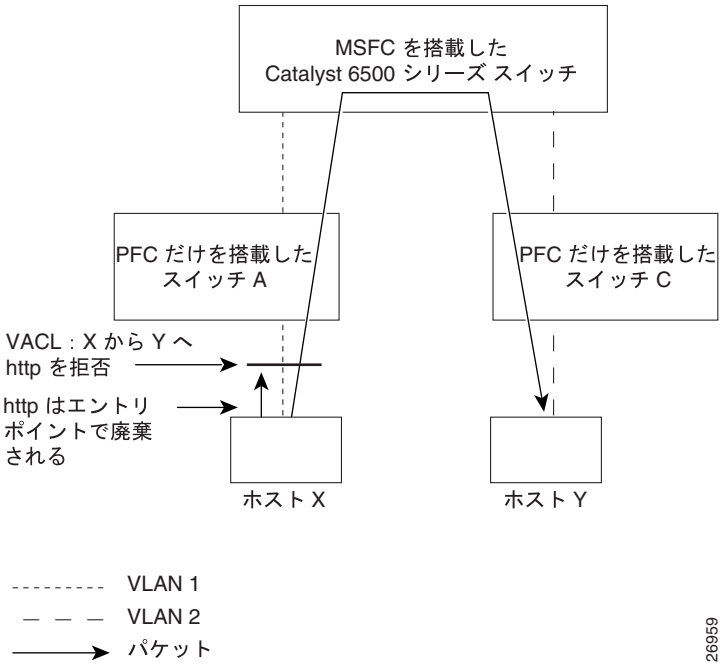
ここでは、VACL の一般的な使用例について説明します。

配線クローゼットの設定

配線クローゼットの設定では、Catalyst 6500 シリーズ スイッチに MSFC（ルータ）が搭載されていないことがあります。この設定では、スイッチにより VACL および QoS ACL がサポートされます。ホスト X およびホスト Y は異なる VLAN 上にあり、配線クローゼットのスイッチ A およびスイッチ C に接続しているとします（図 15-4 を参照）。ホスト X からホスト Y へのトラフィックは、最終的に、MSFC 搭載スイッチによってルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックの入口であるスイッチ A でアクセス制御することができます。

ホスト X からホスト Y への HTTP トラフィックをスイッチングしない場合は、スイッチ A に VACL を設定します。この場合、ホスト X からホスト Y への HTTP トラフィックはすべてスイッチ A で廃棄され、MSFC 搭載スイッチにはブリッジングされません。

図 15-4　配線クローゼットの設定



特定のサーバ ポートへのブロードキャスト トラフィックのリダイレクト

一部のアプリケーション トラフィックは、VLAN 内のすべてのホストに到達するブロードキャスト パケットを使用します。VACL により、これらのブロードキャスト パケットを特定のアプリケーション サーバのポートにリダイレクトできます。

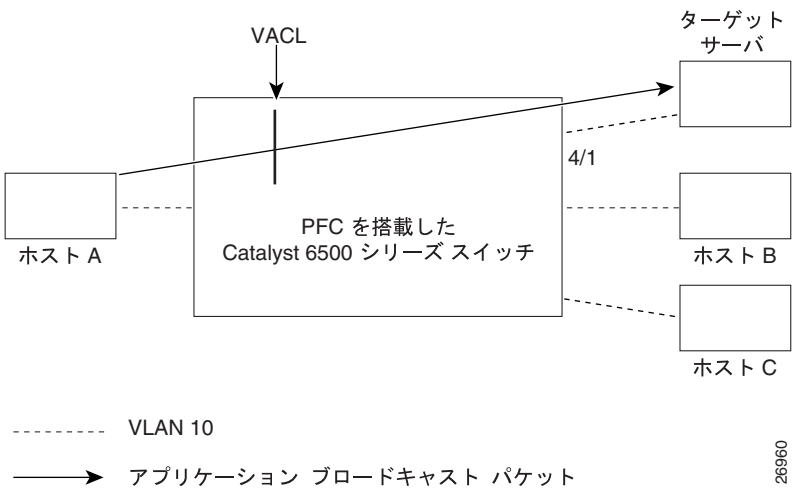
図 15-5 では、ホスト A からアプリケーション ブロードキャスト パケットがターゲットのアプリケーション サーバ ポートにリダイレクトされ、他のポートにパケットは送信されません。

ブロードキャスト トラフィックを特定のサーバ ポートにリダイレクトするには、イネーブル モードで次の作業を行います（対象となるサーバ アプリケーション ポートは、TCP ポート 5000 です）。

	作業	コマンド
ステップ 1	ブロードキャスト パケットをリダイレクトします。	**set security acl ip SERVER redirect 4/1 tcp any host 255.255.255.255 eq 5000**
ステップ 2	他のすべてのトラフィックを許可します。	**set security acl ip SERVER permit ip any any**
ステップ 3	VACL をコミットします。	**commit security acl SERVER**
ステップ 4	VACL を VLAN 10 にマッピングします。	**set security acl map SERVER 10**

（注）　トラフィックをポート グループにリダイレクトすることによって、ブロードキャスト トラフィックをマルチキャストの宛先に送信することができます（図 15-5 を参照）。

図 15-5　特定のサーバ ポートへのブロードキャスト トラフィックのリダイレクト



特定のサーバに対する DHCP 応答の制限

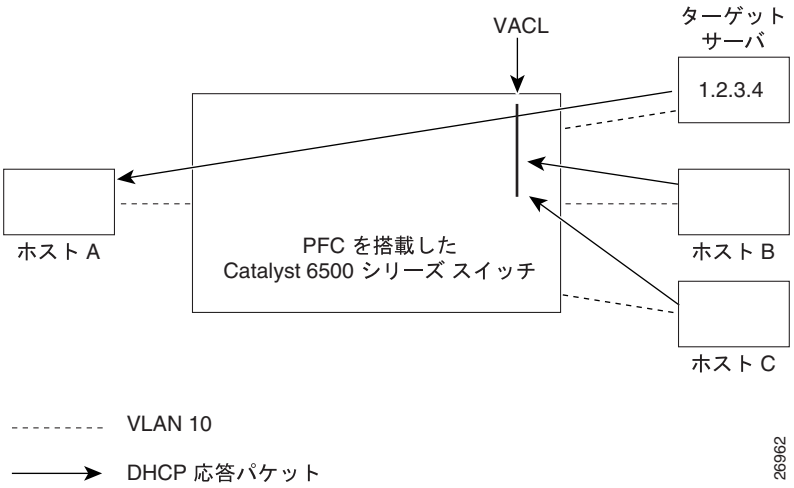
Dynamic Host Configuration Protocol（DHCP）要求がブロードキャストされると、VLAN 内のすべての DHCP サーバに送信されるので、複数の応答が戻されます。VACL によって、*特定の* DHCP サーバからの応答だけを受けるようにし、他の応答を廃棄することができます。

DHCP 応答を特定のサーバに制限するには、イネーブル モードで次の作業を行います（ターゲットの DHCP サーバの IP アドレスは、1.2.3.4 です）。

	作業	コマンド
ステップ 1	ホスト 1.2.3.4 からの DHCP 応答を許可します。	**set security acl ip SERVER permit udp host 1.2.3.4 any eq 68**
ステップ 2	他のホストからの DHCP 応答を拒否します。	**set security acl ip SERVER deny udp any any eq 68**
ステップ 3	他の IP トラフィックを許可します。	**set security acl ip SERVER permit any**
ステップ 4	VACL をコミットします。	**commit security acl SERVER**
ステップ 5	VACL を VLAN 10 にマッピングします。	**set security acl map SERVER 10**

図 15-6 では、DHCP 要求に対して、ターゲット サーバの DHCP 応答だけが戻されています。

図 15-6　特定のサーバの DHCP 応答のリダイレクト



他の VLAN 上のサーバからのアクセス拒否

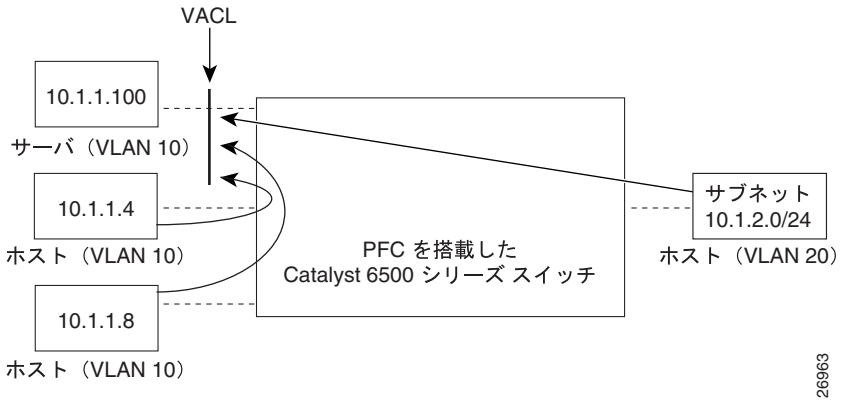
他の VLAN 上のサーバからのアクセスを制限することができます。たとえば、VLAN 10 のサーバ 10.1.1.100 で、次のようなアクセス制限をする必要があるとします（図 15-7 を参照）。

- VLAN 20 のサブネット 10.1.2.0/24 のホストからのアクセスを拒否する
- VLAN 10 のホスト 10.1.1.4 および 10.1.1.8 からのアクセスを拒否する

他の VLAN 上のサーバからのアクセスを拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	サブネット 10.1.2.0/24 のホストからのトラフィックを拒否します。	**set security acl ip SERVER deny ip 10.1.2.0 0.0.0.255 host 10.1.1.100**
ステップ 2	ホスト 10.1.1.4 からのトラフィックを拒否します。	**set security acl ip SERVER deny ip host 10.1.1.4 host 10.1.1.100**
ステップ 3	ホスト 10.1.1.8 からのトラフィックを拒否します。	**set security acl ip SERVER deny ip host 10.1.1.8 host 10.1.1.100**
ステップ 4	他の IP トラフィックを許可します。	**set security acl ip SERVER permit ip any any**
ステップ 5	VACL をコミットします。	**commit security acl SERVER**
ステップ 6	VACL を VLAN 10 にマッピングします。	**set security acl map SERVER 10**

図 15-7　他の VLAN 上のサーバからのアクセス拒否



ARP トラフィックの制限

（注）　この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

ARP トラフィックは、デフォルトでは各 VLAN 上で許可されます。**set security acl ip** *acl_name* **deny arp** コマンドを使用して、VLAN 単位で ARP トラフィックを拒否することができます。このコマンドを入力すると、ACL をマッピングした VLAN 上で ARP トラフィックが拒否されます。ARP トラフィックを拒否した VLAN 上で、ARP トラフィックを再び許可するには、**set security acl ip** *acl_name* **permit arp** コマンドを入力します。

ARP トラフィックの検査

（注）　この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

ここでは、ARP トラフィック検査機能について説明します。

概要

ARP は認証メカニズムを備えていない簡易プロトコルなので、ARP 要求および応答が正しいかどうかを確認する方法がありません。認証メカニズムがなければ、悪意のあるユーザ / ホストによってレイヤ 2 ネットワークまたはブリッジ ドメインにある同じ VLAN 上の他のホストの ARP テーブルが破壊される可能性があります。

たとえば、ユーザ / ホスト A（悪意のあるユーザ）が、デフォルト ルータの IP アドレスとホスト A の MAC アドレスで、非送信請求 ARP 応答（不必要な ARP パケット）をサブネット上の他のホストに送信することがあります。従来の OS（オペレーティング システム）では、デフォルト ルータのスタティック ARP エントリがホストにすでにある場合でも、ホスト A からの新たにアドバタイズされたバインディングが学習されます。ホスト A が IP 転送をイネーブルにし、「スプーフィングされた」ホストとルータ間ですべてのパケットをやり取りする場合、（たとえば dsniff プログラムを使用した）man-in-the-middle 攻撃を実行できます。このスプーフィングされたホストでは、そのトラフィックのすべてにスニファが行われていることを認識しません。

ARP トラフィック検査によって、セキュリティ ACL（VACL）フレームワーク内に順序依存型の一連のルールを設定して ARP テーブルへの攻撃を防止できます。

実装

VLAN 上の VACL に ARP トラフィック検査の具体的なルールが存在する場合は、すべての ARP パケットは VACL の ACE を介してインデックスによる指定で CPU に送られます。パケットは、ARP トラフィック検査タスクによって指定されたルールへの適合が検査されます。適合パケットは転送されますが、非適合パケットは廃棄されてログが取られます（ロギングがイネーブルの場合）。

ARP トラフィック検査のルールは、次の例に示すように指定された IP アドレスに対して ARP バインディングを指定します。

```
permit arp-inspection host 10.0.0.1 00-00-00-01-00-02
permit arp-inspection host 20.0.0.1 00-00-00-02-00-03
deny arp-inspection host 10.0.0.1 any
deny arp-inspection host 20.0.0.1 any
permit arp-inspection any any
```

上記の一連のルールによって、00-00-00-01-00-02 だけが IP アドレス 10.0.0.1 の MAC アドレスとしてアドバタイズされます。同様に、MAC アドレス 00-00-00-02-00-03 は IP アドレス 20.0.0.1 にバインドされます。10.0.0.1 および 20.0.0.1 のその他の MAC アドレスをアドバタイズする ARP パケットは廃棄されます（3 行めおよび 4 行めの **deny** 動作によって達成）。残りの ARP パケットは通過が許可されます（5 行めの **permit** 動作によって達成）。

ARP トラフィック検査設定時の注意事項

ここでは、ARP トラフィック検査設定時の注意事項について説明します。

- ARP トラフィック検査句を VACL の先頭に表示します。
- VACL に設定できる ARP トラフィック検査句の数の上限は 32 です。
- ARP トラフィック検査句を含んだ ACL の最大文字数は 29 文字です。
- ARP トラフィック検査 ACE は、IP ACE になるように変更できません。その逆も同様です。
- ARP トラフィック検査 ACE は、IP ACE の前に挿入できません。その逆も同様です。
- 同じ VACL で汎用 deny/permit ステートメントを ARP トラフィック検査句と一緒に使用しないでください。汎用 deny/permit ステートメントは、**set security acl ip** *acl_name* {**deny** | **permit**} **arp** コマンドを使用してインストールします。
- MSFC がホストのゲートウェイである場合は、MSFC IP/MAC のバインディングを使用可能にする必要があります。ARP トラフィック検査を実行する場合は、ゲートウェイ IP/MAC バインディングを使用可能にすることを推奨します。
- ARP トラフィック検査は、VACL の既存のロギング機能を使用します。パケットが ARP トラフィック検査ルールを経たあと、結果が [permit] の場合、パケットは宛先 MAC アドレス（またはブロードキャスト アドレス）に転送されます。結果が [deny] の場合は、パケットは廃棄され、VACL ロギング プロセスに送信されます（ロギングがイネーブルの場合）。

VACL ロギングは送信元 MAC アドレスおよび ARP ヘッダーのフィールドを使用して、ロギング フローを定義します。使用するフィールドは、送信元 IP アドレス、送信元 MAC アドレス、および ARP 演算コード（要求、応答）です。

set security acl log maxflow *max_flows* コマンドを入力すると、ログ済みフローの数を制限できます。ただし、**set security acl log ratelimit** *max_rate* コマンドは ARP トラフィック検査ログ済みフローに適用されません。

- RARP パケットはホスト上の ARP エントリの学習に使用されず、ARP を破壊するような害を及ぼすことはありません。PFC2 および PFC3A/PFC3B/PFC3BXL では、ARP および RARP パケットの区別が行われません。CPU への ARP パケットのリダイレクトに使用される ACE も、RARP パケットをリダイレクトします。グローバル レート制限とは、結合 ARP および RARP パケットに対するレート制限のことです。ARP トラフィック検査ルールは RARP パケットには適用されないので、RARP パケットはそのまま転送されます。汎用 ARP deny ステートメントも RARP パケットを拒否します。転送される RARP パケットの数は、**show security acl arp-inspection statistics** コマンドを実行すると表示できます。
- ARP トラフィック検査句を伴う VACL を管理 VLAN（sc0/sc1 インターフェイス）にマッピングすることは、サポートされていません。
- ポートが EtherChannel に組み込まれていたとしても、廃棄およびシャットダウン スレッシュホールドはポートベースのままです。スレッシュホールドは、EtherChannel の形成に必要な*一致*の構成要素ではありません（PAgP は*一致した* EtherChannel リンクを特定すると、そのポートを EtherChannel にまとめます）。
- ハードウェアによる ARP パケットの認識方法が原因で、送信元アドレスが 0.0.0.0、宛先アドレスが 0.0.0.0 の IP パケット、および IP プロトコル ICMP も ARP トラフィック検査タスクにリダイレクトされます。これらのパケットは無効なパケットなので廃棄されます。このようなパケットのカウントは、**show security acl arp-inspection statistics** コマンドの一部として表示されます。
- ARP トラフィック検査タスクによって廃棄されたすべてのパケットについて Syslog メッセージが生成されると、コンソールはメッセージでいっぱいになります。このような状況を避けるため、1 分当たりの許容 Syslog メッセージを 40 に制限します。
- 次に、一般的な設定エラーを回避する例を示します。以下は一般的な ARP トラフィック検査 ACL です。

```
-------------------------------
set security acl ip my_arp
---------------------------------------------------
arp permit
1. permit arp-inspection host 10.6.62.86 00-b0-c2-3b-db-fd
2. deny arp-inspection host 10.6.62.86 any
3. permit arp-inspection any any
---------------------------
```

この ACL によって、MAC アドレス 00-b0-c2-3b-db-fd だけが IP アドレス 10.6.62.86 の MAC アドレスとしてアドバタイズされます。この ACL は、IP ACL に暗黙の ip deny any any があるので、*すべての* IP パケットを拒否します。

すべての IP トラフィックを通過させるには、次のように ACL の末尾に明示的な permit ip any any がなければなりません。

```
--------------------
set security acl ip my_arp
---------------------------------------------------
arp permit
1. permit arp-inspection host 10.6.62.86 00-b0-c2-3b-db-fd
2. deny arp-inspection host 10.6.62.86 any
3. permit arp-inspection any any
4. permit ip any any
----------------------
```

- 次に、ARP トラフィック検査を使用した一般的な設定例を示します。次の ACL を使用して指定された 2 つの IP アドレスを保護し、指定されたもの以外の MAC アドレスでの ARP トラフィック検査を実行しません。

```
set security acl ip ACL_VLAN951 permit arp-inspection host 132.216.251.129
00-d0-b7-11-13-14
set security acl ip ACL_VLAN951 deny arp-inspection host 132.216.251.129 any log
set security acl ip ACL_VLAN951 permit arp-inspection host 132.216.251.250
00-d0-00-ea-43-fc
set security acl ip ACL_VLAN951 deny arp-inspection host 132.216.251.250 any log
set security acl ip ACL_VLAN951 permit arp-inspection any any
set security acl ip ACL_VLAN951 permit ip any any
```

ARP トラフィック検査の設定手順

ここでは、ARP トラフィック検査の設定手順について説明します。

ARP トラフィック検査の設定

- 特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否（p.15-33）
- 特定の IP アドレスのバインディングをアドバタイズする ARP の許可または拒否（p.15-34）
- すべての ARP パケットの許可または拒否（p.15-34）
- 特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否（p.15-35）
- MAC アドレスが一致しないパケットの廃棄（p.15-35）
- MAC または IP アドレスが無効なパケットの廃棄（p.15-36）
- ARP トラフィック検査統計情報の表示（p.15-36）
- ARP トラフィック検査統計情報の消去（p.15-37）

ARP トラフィック検査のレート制限の設定

- グローバル ベースのレート制限の設定（p.15-37）
- ポート単位ベースのレート制限の設定（p.15-38）
- ARP トラフィック検査のための errdisable-timeout オプションの設定（p.15-39）

ARP トラフィック検査のロギングの設定

- ARP トラフィック検査のロギングの設定（p.15-39）

特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否

特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	特定の IP アドレスと MAC アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection host** *ip_address mac_address*
ステップ 2	VACL をコミットします。	**commit security acl** {**acl_name** | **all** | **adjacency**}

次に、IP アドレス 172.20.52.54 と MAC アドレス 00-01-64-61-39-c2 のバインディングをアドバタイズする ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL1 permit arp-inspection host 172.20.52.54
00-01-64-61-39-c2
Operation successful.
Console> (enable) commit security acl ACL1
Console> (enable) ACL commit in progress.

ACL 'ACL1' successfully committed.
```

特定の IP アドレスのバインディングをアドバタイズする ARP の許可または拒否

指定した IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	指定した IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection host** *ip_address* **any**
ステップ 2	VACL をコミットします。	**commit security acl** {**acl_name** | **all** | **adjacency**}

次に、IP アドレス 172.20.52.19 のバインディングをアドバタイズする ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL2 permit arp-inspection host 172.20.52.19 any
Operation successful.
Console> (enable) commit security acl ACL2
Console> (enable) ACL commit in progress.

ACL 'ACL2' successfully committed.
```

すべての ARP パケットの許可または拒否

すべての ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	すべての ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection any any**
ステップ 2	VACL をコミットします。	**commit security acl** {**acl_name** | **all** | **adjacency**}

次に、すべての ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL3 permit arp-inspection any any
Operation successful.
Console> (enable) commit security acl ACL3
Console> (enable) ACL commit in progress.

ACL 'ACL3' successfully committed.
```

特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットの許可または拒否

特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否するには、イネーブル モードで次の作業を行います。

（注）　*ip_mask* は逆マスクです。[0] ビットは「一致」を意味し、[1] ビットは「無視」を意味します。たとえば、10.3.5.6 と 0.0.0.255 は 10.3.5/24 に相当します。

	作業	コマンド
ステップ 1	特定ネットワーク上の IP アドレスのバインディングをアドバタイズする ARP パケットを許可または拒否します。	**set security acl ip** *acl_name* {**permit** | **deny**} **arp-inspection** *ip_address ip_mask* **any**
ステップ 2	VACL をコミットします。	**commit security acl** {*acl_name* | **all** | **adjacency**}

次に、サブネット 10.3.5.0/24 上の IP アドレスのバインディングをアドバタイズする ARP パケットを許可する例を示します。

```
Console> (enable) set security acl ip ACL4 permit arp-inspection 10.3.5.6 0.0.0.255
any
Operation successful.
Console> (enable) commit security acl ACL4
Console> (enable) ACL commit in progress.

ACL 'ACL4' successfully committed.
```

MAC アドレスが一致しないパケットの廃棄

（イーサネット ヘッダーの）送信元イーサネット MAC アドレスが ARP ヘッダーの送信元 MAC アドレスと異なるパケットを廃棄するには、イネーブル モードで次の作業を行います。**drop** キーワードを指定しないと、パケットは廃棄されませんが、Syslog メッセージが表示されます。VACL ロギング機能にパケットを送信するには、**log** キーワードを使用します。

ヒント　通常、**match-mac** 句を使用して ARP スプーフィングを防止しても、各 VLAN の特定 ARP 検査 ACL を作成する必要はなくなりません。**match-mac** 句は、より洗練された ARP テーブル攻撃を受けません。大部分の ARP スプーファは、イーサネット ヘッダーの送信元 MAC アドレスを変更して ARP ペイロードのアドレスを一致させます。

	作業	コマンド
ステップ 1	MAC アドレスの一致しないパケットを識別または廃棄します。	**set security acl arp-inspection match-mac** {**enable** [**drop** [**log**]] | **disable**}
ステップ 2	VACL をコミットします。	**commit security acl** {*acl_name* | **all** | **adjacency**}
ステップ 3	設定を表示します。	**show security acl arp-inspection config**

次に、送信元イーサネット MAC アドレスが ARP ヘッダーの送信元 MAC アドレスと異なるパケットを廃棄する例を示します。

```
Console> (enable) set security acl arp-inspection match-mac enable drop
ARP Inspection match-mac feature enabled with drop option.
Console> (enable)

Console> (enable) show security acl arp-inspection config
Match-mac feature is enabled with drop option.
Console> (enable)
```

MAC または IP アドレスが無効なパケットの廃棄

次の MAC アドレスは無効です。

- 00-00-00-00-00-00
- マルチキャスト MAC アドレス（48 番めのビットを設定）
- ff-ff-ff-ff-ff-ff（これは特殊なケースのマルチキャスト MAC アドレスです）

次の IP アドレスは無効です。

- 0.0.0.0
- 255.255.255.255
- クラス D（マルチキャスト）IP アドレス

MAC または IP アドレスが無効なパケットを廃棄するには、イネーブル モードで次の作業を行います（**drop** キーワードを指定しないと、パケットは廃棄されませんが、Syslog メッセージが表示されます）。

	作業	コマンド
ステップ 1	MAC または IP アドレスが無効なパケットを廃棄します。	**set security acl arp-inspection address-validation** {**enable** [**drop** [**log**]] | **disable**}
ステップ 2	VACL をコミットします。	**commit security acl** {*acl_name* | **all** | **adjacency**}
ステップ 3	設定を表示します。	**show security acl arp-inspection config**

次に、MAC または IP アドレスが無効なパケットを廃棄する例を示します。

```
Console> (enable) set security acl arp-inspection address-validation enable drop
ARP Inspection address-validation feature enabled with drop option.
Console> (enable)

Console> (enable) show security acl arp-inspection config
Address-validation feature is enabled with drop option.
Console> (enable)
```

ARP トラフィック検査統計情報の表示

ARP トラフィック検査タスクによって許可および拒否されたパケットの数を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ARP トラフィック検査タスクによって許可および拒否されたパケットの数を表示します。	**show security acl arp-inspection statistics** [*acl_name*]

（注）　**show security acl** コマンドを入力すると、特定の ARP トラフィック検査設定情報を表示します。

次に、ARP トラフィック検査タスクによって許可および拒否されたパケットの数を表示する例を示します。

```
Console> (enable) show security acl arp-inspection statistics
ARP Inspection statistics
Packets forwarded = 0
Packets dropped = 0
RARP packets (forwarded) = 0
Packets for which Match-mac failed = 0
Packets for which Address Validation failed = 0
IP packets dropped = 0
Console> (enable)
```

ARP トラフィック検査統計情報の消去

ARP トラフィック検査統計情報を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
ARP トラフィック検査統計情報を消去します。	**clear security acl arp-inspection statistics** [*acl_name*]

オプションの引数なしでコマンドを入力すると、すべての ACL で ARP トラフィック検査グローバル統計情報カウンタおよび ARP トラフィック検査統計情報カウンタが消去されます。オプションの引数 *acl_name* を指定すると、特定 ACL の ARP トラフィック検査統計情報だけが消去されます。

（注）　**clear security acl** コマンドを入力すると、ARP トラフィック検査の設定値が消去されます。

グローバル ベースのレート制限の設定

グローバルにスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を実行できます。デフォルトでは、ARP トラフィック検査のトラフィックは 500 パケット / 秒にレート制限されます。最小値は 1 パケット / 秒、最大値は 1000 パケット / 秒です。Supervisor Engine 720 の場合、ハードウェアにより決められる最小値は 10 パケット / 秒です（1 ～ 9 の値は 10 に設定されます）。レート制限をディセーブルにするには、値を 0 に設定します。

（注）　レート制限は、複数の機能で共有されます。レート制限を共有する機能を表示するには、**show security acl feature ratelimit** コマンドを入力します。

グローバル ベースでスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行うには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	グローバル ベースでスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行います。	**set security acl feature ratelimit** *rate*
ステップ 2	グローバル レート制限値を表示します。	**show security acl feature ratelimit**
ステップ 3	スイッチ プロセッサおよび Route Processor（RP; ルート プロセッサ）で設定された、すべてのレート リミッタ設定を表示します。	**show rate-limit**

次に、CPU に送信される ARP トラフィック検査パケットの数を 1000 にレート制限する例を示します。

```
Console> (enable) set security acl feature ratelimit 1000
Dot1x DHCP and ARP Inspection global rate limit set to 1000 pps.
Console> (enable)

Console> (enable) show security acl feature ratelimit
Rate limit value in packets per second = 1000
Protocols set for rate limiting = Dot1x DHCP, ARP Inspection
Console> (enable)

Console> (enable) show rate-limit
Configured Rate Limiter Settings:

Rate Limiter Type    Status  Rate (pps)     Burst
-------------------- ------  -------------- -----
VACL LOG             On      2500           1
ARP INSPECTION       On      1000           1
FIB RECEIVE          Off     *              *
FIB GLEAN            Off     *              *
L3 SEC FEATURES      Off     *              *

Console> (enable)
```

ポート単位ベースのレート制限の設定

ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を実行できます。レートが **drop-threshold** を超える場合、超過パケットは廃棄されます（さらに **shutdown-threshold** 制限に対してカウントされます）。レートが **shutdown-threshold** を超える場合は、*mod/port* によって指定されたポートはシャットダウンされます。デフォルトでは、両方のスレッシュホールド値が 0 です（ポート単位のレート制限は適用されません）。両方のスレッシュホールドの最大値は 1000 パケット / 秒（pps）です。

ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行うには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数に対してレート制限を行います。	**set port arp-inspection** *mod/port* **drop-threshold** *packets_per_second* **shutdown-threshold** *packets_per_second* **set port arp-inspection** *mod/port* **drop-threshold** *packets_per_second* **set port arp-inspection** *mod/port* **shutdown-threshold** *packets_per_second*

	作業	コマンド
ステップ 2	廃棄およびシャットダウン スレッシュホールドを表示します。	**show port arp-inspection** {[*mod/port*] | [*mod*]}

次に、ポート単位でスーパバイザ エンジン CPU に送信される ARP トラフィック検査パケットの数をレート制限する例を示します。ポート 3/1 に対して廃棄スレッシュホールドを 700、シャットダウン スレッシュホールドを 800 に設定します。

```
Console> (enable) set port arp-inspection 3/1 drop-threshold 700 shutdown-threshold
800
Drop Threshold=700, Shutdown Threshold=800 set on port 3/1.
Console> (enable)

Console> (enable) show port arp-inspection 3/1
Port                       Drop Threshold Shutdown Threshold
-------------------------  -------------- ------------------
 3/1                                  700                800
Console> (enable)
```

ARP トラフィック検査のための errdisable-timeout オプションの設定

set errdisable-timeout {**enable** | **disable**} **arp-inspection** コマンドを使用して、ARP トラフィック検査のために errdisable-timeout オプションを設定できます。errdisable-timeout オプションの詳細については、「ポートの errdisable ステートにおけるタイムアウト設定」（p.4-13）を参照してください。

ARP トラフィック検査のロギングの設定

ロギング オプションを設定して廃棄される ARP トラフィック検査パケットのログを取るには、イネーブル モードで次の作業を行います。

作業	コマンド
廃棄される ARP トラフィック検査パケットのログを取ります。	**set security acl ip** *acl_name* **deny arp-inspection** {**host** *ip_address* {**any** | *mac_address*} | *ip_address* *ip_mask* **any** | **any any**} [**log**]

VACL ロギング オプションの詳細については、「VACL ロギングの設定」（p.15-60）を参照してください。ここでは、**set security acl log maxflow** *max_number* コマンドによるログ フローの数の制限についても説明します。

ロギングされた ARP トラフィック検査パケットを表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ロギングされた ARP トラフィック検査パケットを表示します。	**show security acl log flow arp** [**host** *ip_address* [**vlan** *vlan*]]

オプションの **host** *ip address* を指定すると、指定したホストの IP アドレスのバインディングをアドバタイズする ARP パケットだけが表示されます。オプションの **vlan** *vlan* を指定した場合は、検索が指定した VLAN に限定されます。

ダイナミック ARP 検査

（注）Dynamic ARP Inspection（DAI）を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 のみです。

ここでは、DAI について説明します。

- 概要（p.15-40）
- ダイナミック ARP 検査の設定手順（p.15-42）

概要

DAI では、バインディングのアドバタイズを適用するのに DHCP スヌーピングで作成されたバインディング情報を使用して、[man-in-the-middle] 攻撃を防ぎます。これらの攻撃では、攻撃者が通信データを代行受信し、それを選択的に変更して通信アソシエーション内の 1 つまたは複数のエントリになりすまします。DAI では、ARP パケットの MAC アドレスおよび IP アドレスが、同一 VLAN 内にある既存の DHCP スヌーピング バインディングと一致することを確認することで、セキュリティ用の特別レイヤを ARP 検査に追加します。DHCP バインディングが存在することを確認する追加のチェックを除いて、ARP 検査の基本的な機能とパケット フローは変わりません（論理フローチャートについては図 15-8 を参照してください）。

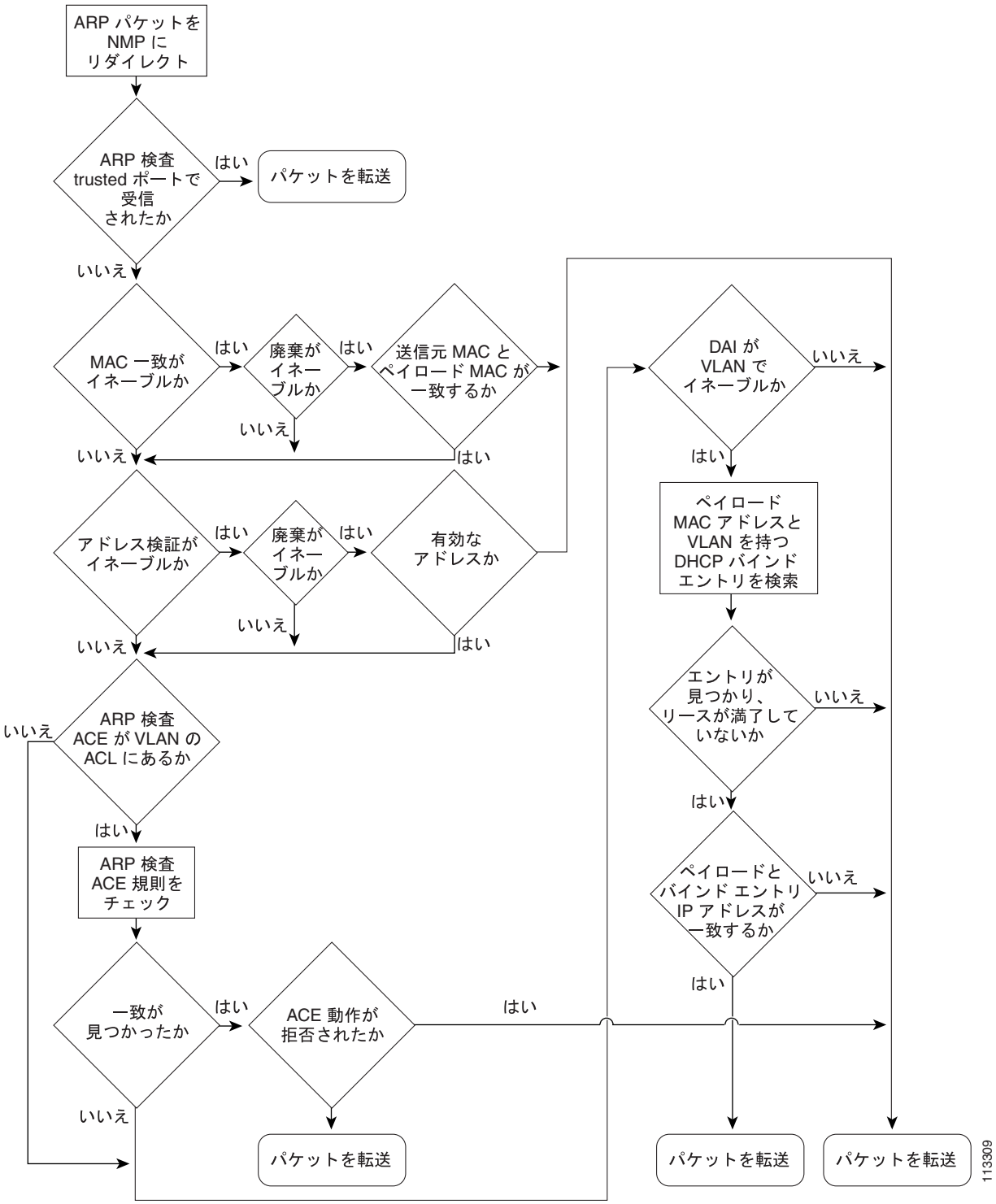
（注）untrusted（信頼性がない）ポートから送信される ARP パケットのみが検査されます。trusted（信頼性のある）ポートから受信した ARP パケットは、検査なしに転送されます（このプロセスは、スタティックおよびダイナミック ARP 検査の両方に適用されます）。デフォルトで、システムは MAFC ポートを ARP 検査 trusted ポートとして設定します。

セキュリティ ACL を作成する場合、静的に設定された ARP 検査規則は DHCP バインディングの DAI チェックよりもプライオリティが高いので、注意が必要です。発生したことに対するチェックができなくなるので、**permit arp-inspection any any** 句をセキュリティ ACL に配置しないでください。

DAI を VLAN 単位でイネーブルまたはディセーブルに設定できます。DAI ポートを untrusted と設定する場合、その DAI ポートを DHCP スヌーピング untrusted ポートとしても設定する必要があります。DAI がイネーブルになっているすべての VLAN で、DHCP スヌーピングをイネーブルにする必要があります。オプションで、DAI で拒否された ARP パケットに対するロギングをイネーブルにできます。

（注）すべての（またはほとんどの）IP アドレスの割り当てが DHCP を使用して実行されている VLAN でイネーブルにした場合に、DAI がもっともよく機能します。

図 15-8　ダイナミック ARP 検査のフロー チャート



注意　管理 VLAN sc0 および sc1 で DAI をイネーブルにできません。

スタティック IP アドレス割り当てが VLAN にある場合、関連ポートを ARP 検査の trusted ポートに設定するか、またはスタティック ARP 検査でこれらの MAC アドレスおよび IP アドレスを許可するように設定する必要があります。

ダイナミック ARP 検査の設定手順

（注）　DAI、DHCP スヌーピング、および IP 送信元ガードを使用する場合、ハイ アベイラビリティをイネーブルにすることを推奨します。ハイ アベイラビリティがイネーブルでない場合、スイッチオーバー後にこれらの機能が動作するようにクライアントは IP アドレスを更新する必要があります。DHCP スヌーピングおよび IP 送信元ガードの設定の詳細については、第 32 章「DHCP スヌーピングおよび IP ソース ガードの設定」を参照してください。

DAI を設定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	VLAN で DAI をイネーブルにします。	**set security acl arp-inspection dynamic** {**enable** | **disable**} {*vlanlist*}
ステップ 2	ARP パケットの検査をイネーブルまたはディセーブルにします。	**set port arp-inspection** *portlist* **trust** {**enable** | **disable**}
ステップ 3	DAI が拒否したパケットのロギングをイネーブルにします。 （注）　スタティック ARP 規則拒否のロギングは、引き続き規則（ACE）CPG で制御されます。	**set security acl arp-inspection dynamic log** {**enable** | **disable**}
ステップ 4	DAI および DAI ロギング設定を確認します。	**show security acl arp-inspection config**

次に、VLAN 100 で DAI をイネーブルにする例を示します。

```
Console> (enable) set security acl arp-inspection dynamic enable 100
Dynamic ARP Inspection is enabled for vlan(s) 100.
Console> (enable) set port arp-inspection 2/2 trust enable
Port(s)  2/2 state set to trusted for ARP Inspection.
Console> (enable) set security acl arp-inspection dynamic log enable
Dynamic ARP Inspection logging enabled.
Console> show security acl arp-inspection config
Match-mac feature is disabled.
Address-validation feature is disabled.
Dynamic ARP Inspection is disabled on vlan(s) 1,1006-1013.
Dynamic ARP Inspection is enabled on vlan(s) 100.
Logging for Dynamic ARP Inspection rules is enabled.
Console>
```

プライベート VLAN 上での ACL の設定

プライベート VLAN により、プライマリ VLAN をサブ VLAN（セカンダリ VLAN）に分割し、コミュニティ VLAN または独立 VLAN として設定できます。Release 6.1(1) より前のソフトウェア リリースでは、ACL を設定できるのはプライマリ VLAN 上だけなので、ACL はすべてのセカンダリ VLAN に適用されます。Release 6.1(1) 以降のソフトウェア リリースでは、ACL の適用は次のようになります。

- VACL を、セカンダリ VLAN またはプライマリ VLAN にマッピングできます。
- プライマリ VLAN にマッピングした Cisco IOS ACL が、関連付けられたセカンダリ VLAN にマッピングされます。
- Cisco IOS ACL を、セカンダリ VLAN にマッピングすることはできません。

- ダイナミック ACE を、プライベート VLAN にマッピングすることはできません。
- QoS ACL を、セカンダリ VLAN またはプライマリ VLAN にマッピングできます。

VACL をプライマリ VLAN にマッピングした場合、ルータからホストへのトラフィックがフィルタリングされます。また、セカンダリ VLAN にマッピングした場合は、ホストからルータへのトラフィックがフィルタリングされます。

（注）Release 6.2(1) 以降のソフトウェア リリースでは、MSFC 混合ポートを通ってトラフィックがプライベート VLAN の境界を越えるとき、双方向コミュニティ VLAN を使用してプライマリ VLAN からセカンダリ VLAN への逆マッピングを実行できます。発信と着信の両方のトラフィックは、VLAN ベースの VACL をコミュニティ（または顧客）単位で両方向に適用できる同一の VLAN で伝送できます。

（注）プライベート VLAN の詳細については、「スイッチ上でのプライベート VLAN の設定」（p.11-22）を参照してください。

トラフィック フローのキャプチャ

設定の詳細については、「特定ポート上でのトラフィック フローのキャプチャ」（p.15-58）を参照してください。

サポートされない機能

（注）Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

ここでは、Catalyst 6500 シリーズ スイッチがサポートしていない、またはサポートが制限されている ACL 関連機能について説明します。

- non-IP version 4/non-IPX Cisco IOS ACL — 次のタイプの Cisco IOS セキュリティ ACL は、スイッチのハードウェアで実行することはできません。そのため、MSFC が ACL をソフトウェアで処理することになり、システムのパフォーマンスを*著しく*低下させます。
  - ブリッジ グループ ACL
  - IP アカウンティング
  - 着信 / 発信のレート制限
  - 送信元ノード番号を指定した標準 IPX
  - 送信元ノード番号またはソケット番号を指定した IPX 拡張アクセス リストは、ハードウェアでは実行できません。
  - 標準 XNS アクセス リスト
  - 拡張 XNS アクセス リスト
  - DECnet アクセス リスト
  - 拡張 MAC アドレス アクセス リスト
  - プロトコル タイプコード アクセス リスト
- ヘッダー長が 5 未満の IP パケットは、アクセス制御されません。
- full flow IPX VACL の非サポート — IPX VACL は、送信元 / 宛先ネットワーク番号、パケットタイプ、宛先ノード番号だけを指定したフローを対象にしています。IPX フローの指定では、送信元ノード番号およびソケット番号はサポートされません。

VACL の設定

ここでは、VACL の設定方法について説明します。設定の作業を行う前に、「VACL 設定時の注意事項」（p.15-45）を参照してください。

ここでは、VACL 設定時の注意事項と要約について説明します。

VACL 設定時の注意事項

ここでは、VACL 設定時の注意事項について説明します。

注意　ACL の変更はすべて、編集バッファに一時的に保存されます。すべての ACE を NVRAM（不揮発性 RAM）にコミットするには、**commit** コマンドを入力する必要があります。ACE を指定せずにコミットした ACL は、削除されます。ACE をまとめて入力し、**commit** コマンドを使用してすべての変更を NVRAM に保存することを推奨します。

（注）　Cisco IOS ACL と VACL は、NVRAM ではなくフラッシュ メモリから設定できます。詳細については、「VACL および QoS ACL の設定およびフラッシュ メモリへの保存」（p.15-67）を参照してください。

（注）　Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

- 「同一 VLAN インターフェイス上に Cisco IOS ACL および VACL を設定する場合の注意事項」（p.15-18）を参照してください。
- 設定例については、「ネットワークでの VACL の使用」（p.15-27）を参照してください。
- 「サポートされない機能」（p.15-44）を参照してください。
- 「ACL マージ アルゴリズムの指定」（p.15-47）を参照してください。
- VLAN にマッピングするには、まず VACL をコミットする必要があります。デフォルトの VACL はありません。また、VACL/VLAN のデフォルト マッピングもありません。
- ルーテッド VLAN インターフェイス（入力または出力）上のトラフィックを拒否する Cisco IOS ACL が設定されておらず、かつ VACL が設定*されていない*場合、すべてのトラフィックが許可されます。
- ACL では、ACE の入力順序が重要になります。スイッチに入ってくるパケットは、まず ACL の最初の ACE と照合されます。一致しない場合、パケットはリストの次の ACE と照合されます。どの ACE とも一致しない場合、パケットは拒否（廃棄）されます。

- 編集バッファの内容を変更する前に、必ず **show security acl info** *acl_name* **editbuffer** コマンドを使用して、*現在の* ACE リストを確認してください。
- 冗長 MSFC を搭載したシステムでは、両方の MSFC 上で、Cisco IOS ACL および VACL の同じ ACL 設定を適用する必要があります。
- ACL をコミットしないで削除した場合、システムの ACL の最大数が誤って算出されることがあります。
- **show security acl resource-usage** および **show qos acl resource-usage** コマンドの出力では、ハードウェアに ACL を保存できるスペースがなくなっても、使用率が 100 % にならないことがあります。ACL 管理者が必要に応じてクリーンアップおよびマッピングを実行できるように、予備の ACL スペースが確保されているためです。
- 非常に多数の ACL を設定すると、システムの起動時間が通常より長くなることがあります。
- リダイレクト オプションを使用する場合、次の注意事項に留意してください。
  - リダイレクト パケットを送出できるのは、そのトラフィックが属している VLAN をサポートしているポートだけです。
  - リダイレクト オプションの動作は、パケットを受信してリダイレクト ポートに送信するだけで、ルーティングは実行しません。
  - パケットが多数の VLAN から送信される場合、リダイレクト ポートはこれらの VLAN をフォワーディング ステートにする必要があります。ポートで複数の VLAN をサポートするには、リダイレクト ポートをトランクとして設定しなければならないことがあります。
  - ルーティングされていないトラフィックを受信できるように、キャッシュは混合（promiscuous）モードに設定します。
  - 複数のポートにトラフィックを転送して基本的な VLAN ベースのロードバランシングを実行するには、リダイレクト オプションを使用します。各ポートは、そのポートでフォワーディング ステートになっている VLAN のパケットだけを転送します。

VACL 設定の要約

VACL を作成して、VLAN にマッピングする手順は、次のとおりです。

ステップ 1　**set security acl ip** コマンドを入力して VACL を作成し、ACE を追加します。

ステップ 2　**commit** コマンドを入力して、VACL および関連付けられた ACE を NVRAM にコミットします。

ステップ 3　**set security acl map** コマンドを入力して、VACL を VLAN にマッピングします。

（注）　この説明では IP VACL を使用していますが、同じ手順で IPX および non-IP version 4/non-IPX VACL を設定することもできます。

（注）　VACL はリストの末尾に暗黙の拒否ステートメントが付加されるので、どの VACL ACE にも一致しないパケットは拒否されます。

CLI からの VACL の設定

ここでは、Catalyst 6500 シリーズ スイッチ上で VACL を作成し、アクティブにする手順について説明します。これらの作業は、実行する順序に従って記載されています。

ここで説明する作業は、次のとおりです。

ACL マージ アルゴリズムの指定

ACL マージ アルゴリズムには、BDD と ODM の 2 種類があります。ODM は、Release 7.1(1) で採用された拡張アルゴリズムです。BDD アルゴリズムは、Release 7.1(1) より前のソフトウェア リリースで使用されていました。ODM を使用した場合、マージ後の ACE は順序に依存します。BDD を使用した場合、マージ後の ACE は順序には関係ありません。

（注）Release 8.1(1) 以降のソフトウェア リリースでは、BDD アルゴリズムはどのプラットフォーム（PFC、PFC2、または PFC3A/PFC3B/PFC3BXL）上でもサポートされなくなりました。デフォルトの ACL マージ アルゴリズムは ODM です。Release 8.1(1) 以降のソフトウェア リリースでは、コマンドが次のように変更されています。**set aclmerge algo** および **set aclmerge bdd** コマンドは削除されました。**show aclmerge** {**bdd** | **algo**} コマンドは **show aclmerge algo** になりました。

（注）ODM アルゴリズムの例については、「Release 7.1(1) 以降のスーパバイザ エンジン ソフトウェア リリースの場合のマージ結果の推定」（p.15-23）を参照してください。

デフォルトのアルゴリズムは ODM です。BDD をディセーブルにした場合、マージ アルゴリズムは ODM だけになります。BDD がイネーブルの場合、BDD アルゴリズムまたは ODM アルゴリズムのどちらか一方を選択できます。ACL マージ アルゴリズムを変更するには、BDD がイネーブルでなければなりません。BDD をイネーブルまたはディセーブルするには、**set aclmerge bdd** コマンドを使用します。BDD をイネーブルまたはディセーブルにした場合、その変更が有効になるのは、システムの再起動後です。

注意　64 MB DRAM が搭載されたスーパバイザ エンジン上で BDD をイネーブルにすると、メモリが不足する可能性があります。これを防ぐためには、メモリを 128 MB にアップグレードするか、BDD をディセーブルにする必要があります。

選択した ACL マージ アルゴリズムは、すべての新規 ACL マージで有効です。設定済みの ACL が変更されることはなく、ACL のマージ時に有効だった ACL マージ アルゴリズムが使用されます。

BDD をイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	BDD をイネーブルまたはディセーブルにします。	**set aclmerge bdd** {**enable** | **disable**}
ステップ 2	現在の BDD ステータス、および次回のシステム再起動時に BDD がイネーブルになるのかディセーブルになるのかを表示します。	**show aclmerge** {**bdd** | **algo**}

次に、BDD をディセーブルにする例を示します。

```
Console> (enable) set aclmerge bdd disable
Bdd will be disabled on system restart.
Console> (enable)
```

次に、現在の BDD ステータス、および次回のシステム再起動時に BDD がイネーブルまたはディセーブルのいずれになるのかを表示する例を示します。

```
Console> (enable) show aclmerge bdd
Bdd is not enabled.
On system restart bdd will be disabled.
Console> (enable)
```

ACL マージ アルゴリズムを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	ACL マージ アルゴリズムを指定します。	**set aclmerge algo** {**bdd** | **odm**}
ステップ 2	現在使用中の ACL マージ アルゴリズムを表示します。	**show aclmerge** {**bdd** | **algo**}

次に、ODM アルゴリズムを指定する例を示します。

```
Console> (enable) set aclmerge algo odm
Acl merge algorithm set to odm.
Console> (enable)
```

次に、現在使用中の ACL マージ アルゴリズムを表示する例を示します。

```
Console> (enable) show aclmerge algo
Current acl merge algorithm is odm.
Console> (enable)
```

IP VACL の作成および ACE の追加

新しい IP VACL を作成して ACE を追加したり、既存の IP VACL に ACE を追加するには、イネーブル モードで次の作業を行います。

作業	コマンド
IP プロトコルを指定する必要がない場合は、この構文を使用します。	**set security acl ip** {*acl_name*} {**permit** | **deny**} {*src_ip_spec*} [**capture**][**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**[1]]
IP プロトコルを指定する場合は、この構文を使用します。	**set security acl ip** {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_ip_spec*} {*dest_ip_spec*} [**precedence** *precedence*] [**tos** *tos*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*] [**log**[1]]

1. **log** キーワードは、拒否された IP VACL のメッセージを記録するだけです。

次に、IPACL1 に 1 つの ACE を作成し、送信元アドレス 172.20.53.4 からのトラフィックを許可する例を示します。

```
Console> (enable) set security acl ip IPACL1 permit host 172.20.53.4 0.0.0.0
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

（注）　VACL はリストの末尾に暗黙の拒否ステートメントが付加されるので、他のトラフィックはすべて拒否されます。

次に、IPACL1 に 1 つの ACE を作成して、すべての送信元アドレスからのトラフィックを許可する例を示します。

```
Console> (enable) set security acl ip IPACL1 permit any
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、IPACL1 に 1 つの ACE を作成して、送信元アドレス 171.3.8.2 からのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl ip IPACL1 deny host 171.3.8.2
IPACL1 editbuffer modified.  Use 'commit' command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL1 editbuffer
set security acl ip IPACL1
-----------------------------------------------------------------
1. permit ip host 172.20.53.4 any
2. permit ip any any
3. deny ip host 171.3.8.2 any
Console> (enable)
```

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPACL1 is committed to hardware.
Console> (enable)
```

（注）　**commit security acl all** コマンドの詳細については、「ACL のコミット」(p.15-54) を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info IPACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

次に、IPACL2 に 1 つの ACE を作成して送信元アドレス 172.20.3.2 からのトラフィックをブロックし、この ACE を VACL の ACE 番号 2 の前に挿入する例を示します。任意で、**modify** キーワードを入力して、既存の ACE を新しい ACE に置き換えることができます。NVRAM に保存されている現在の ACE リストを表示するには、**show security acl info** *acl_name* [**editbuffer**] コマンドを使用します（編集バッファの内容を表示する場合、**editbuffer** キーワードを指定します）。

```
Console> (enable) set security acl ip IPACL2 deny host 172.20.3.2 before 2
IPACL2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、IPACL2 に 1 つの ACE を作成して、送信元アドレスが 1.2.3.4 で宛先アドレスが 255.255.255.255 からの IP トラフィックを、ポート 3/1 にリダイレクトする例を示します。送信元および送信元ワイルドカード 0.0.0.0 の省略形として host を使用できます。また、この ACE は、次の内容も指定しています。

- **precedence —** IP precedence 値です。優先度は、0（ゼロ）が最も低く、7 が最も高くなります。
- **tos —** Type of Service（ToS; サービス タイプ）のレベルで、0 ～ 15 を指定します。

（注）　ToS 値は IP To S バイトのビット 3 ～ 6 です（RFC 1349 により定義）。precedence 値はビット 0 ～ 2 です（RFC 791 により定義）。

```
Console> (enable) set security acl ip IPACL2 redirect 3/1 ip 1.2.3.4 0.0.0.255 host
255.255.255.255 precedence 1 tos min-delay
IPACL2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL2 editbuffer
set security acl ip IPACL2
----------------------------------------------------------------
1. deny 172.20.3.2
2. redirect 1.2.3.4
Console> (enable)
```

（注）　**show security acl info** コマンドの詳細については、「VACL の内容の表示」（p.15-55） を参照してください。

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPACL2 is committed to hardware.
Console> (enable)
```

（注）　**commit security acl all** コマンドの詳細については、「ACL のコミット」（p.15-54）を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info IPACL2** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

IPX VACL の作成および ACE の追加

（注）　Supervisor Engine 720（PFC3A/PFC3B/PFC3BXL）および Supervisor Engine 32（PFC3B/PFC3BXL）では、IPX ルーティングはソフトウェアにより行われ、IPX Cisco IOS ACL および IPX VACL はサポートされません。MAC VACL を使用して IPX パケットを一致させることができます。IPX ARPA フレームを一致させるため、**ipx-arpa** キーワードを入力できます。IPX 非 ARPA フレームおよび Ethertype 0xffff のフレームで一致させるには、0xffff Ethertype を使用します。MAC VACL の設定については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」（p.15-53）を参照してください。

新しい IPX VACL を作成して ACE を追加したり、既存の IPX VACL に ACE を追加するには、イネーブル モードで次の作業を行います。

作業	コマンド
新しい IPX VACL を作成して ACE を追加するか、既存の IPX VACL に ACE を追加します。	**set security acl ipx** {*acl_name*} {**permit** | **deny** | **redirect** *mod_num/port_num*} {*protocol*} {*src_net*} [*dest_net.*[*dest_node*] [[*dest_net_mask.*]*dest_node_mask*]] [**capture**] [**before** *editbuffer_index* **modify** *editbuffer_index*]

次に、IPXACL1 に 1 つの ACE を作成して、送信元ネットワーク 1234 からのすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl ipx IPXACL1 deny any 1234
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、IPXACL1 に 1 つの ACE を作成して、宛先アドレスが 1.A.3.4 のすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl ipx IPXACL1 deny any any 1.A.3.4
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、IPXACL1 に 1 つの ACE を作成して、送信元ネットワーク 3456 からのブロードキャスト トラフィックをポート 4/1 にリダイレクトする例を示します。

```
Console> (enable) set security acl ipx IPXACL1 redirect 4/1 any 3456
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPXACL1 editbuffer
set security acl ipx IPXACL1
-----------------------------------------------------------------
1. deny any 1234
2. deny any any 1.A.3.4
3. redirect 4/1 any 3456
Console> (enable)
```

（注）　**show security acl info** コマンドの詳細については、「VACL の内容の表示」（p.15-55）を参照してください。

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPXACL1 is committed to hardware.
Console> (enable)
```

変更がコミットされたかどうかを確認するには、**show security acl info IPXACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

次に、IPXACL1 に 1 つの ACE を作成して送信元ネットワーク 1 からのすべてのトラフィックを許可し、この ACE を ACE 番号 2 の前に挿入する例を示します。

```
Console> (enable) set security acl ipx IPXACL1 permit any 1 before 2
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、IPXACL1 に 1 つの ACE を作成して、すべての送信元アドレスからのトラフィックを許可する例を示します。

```
Console> (enable) set security acl ipx IPXACL1 permit any any
IPXACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info IPXACL1 editbuffer
set security acl ipx IPXACL1
-----------------------------------------------------------------
1. deny any 1234
2. permit any 1
3. deny any any 1.A.3.4
4. redirect 4/1 any 3456
5. permit any any
ACL IPXACL1 Status: Not Committed
Console> (enable)
```

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL IPXACL1 is committed to hardware.
Console> (enable)
```

（注）　**commit security acl all** コマンドの詳細については、「ACL のコミット」（p.15-54）を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info IPXACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加

注意　IP トラフィックおよび IPX トラフィックは、MAC VACL ではアクセス制御されません。その他のトラフィック タイプ（AppleTalk、DECnet など）はすべて MAC トラフィックとして分類され、MAC VACL によってアクセス制御されます。

新しい non-IP version 4/non-IPX VACL を作成して ACE を追加したり、既存の non-IP version 4/non-IPX VACL に ACE を追加したりするには、イネーブル モードで次の作業を行います。

作業	コマンド
新しい non-IP version 4/non-IPX VACL を作成して ACE を追加するか、既存の non-IP version 4/non-IPX VACL に ACE を追加します。	**set security acl mac** {*acl_name*} {**permit** | **deny**} {*src_mac_addr_spec*} {*dest_mac_addr_spec*} [*ethertype*] [**capture**] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

次に、MACACL1 に 1 つの ACE を作成して、8-2-3-4-7-A からのすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl mac MACACL1 deny host 8-2-3-4-7-A any
MACACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、MACACL1 に 1 つの ACE を作成して、A-B-C-D-1-2 を宛先とするすべてのトラフィックをブロックする例を示します。

```
Console> (enable) set security acl mac MACACL1 deny any host A-B-C-D-1-2
MACACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、MACACL1 に 1 つの ACE を作成して、すべての送信元からのトラフィックを許可する例を示します。

```
Console> (enable) set security acl mac MACACL1 permit any any
MACACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、編集バッファの内容を表示する例を示します。

```
Console> (enable) show security acl info MACACL1 editbuffer
set security acl mac MACACL1
-----------------------------------------------------------------
1. deny 8-2-3-4-7-A any
2. deny any A-B-C-D-1-2
3. permit any any
Console> (enable)
```

（注）　**show security acl info** コマンドの詳細については、「VACL の内容の表示」（p.15-55）を参照してください。

次に、ACE を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl all
ACL commit in progress.
ACL MACACL1 is committed to hardware.
Console> (enable)
```

（注）　**commit security acl all** コマンドの詳細については、「ACL のコミット」（p.15-54）を参照してください。

変更がコミットされたかどうかを確認するには、**show security acl info MACACL1** コマンドを入力します。この VACL が VLAN にマッピングされていない場合には、**set security acl map** コマンドを使用して VLAN にマッピングします。

ACL のコミット

すべての ACL または指定した ACL を NVRAM にコミットするには、**commit** コマンドを使用します。ACE が設定されていない ACL は、コミットしても削除されます。

ACL を NVRAM にコミットするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL を NVRAM にコミットします。	**commit security acl** *acl_name* | **all**

次に、セキュリティ ACL を指定して、NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl IPACL2
ACL commit in progress.
ACL IPACL2 is committed to hardware.
Console> (enable)
```

VACL の VLAN へのマッピング

VACL を VLAN にマッピングするには、**set security acl map** コマンドを使用します。デフォルトの ACL/VLAN マッピングは設定されていないことに注意してください。すべての VACL を VLAN にマッピングする必要があります。

VACL を VLAN にマッピングするには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL を VLAN にマッピングします。	**set security acl map** *acl_name vlans*

次に、IPACL1 を VLAN 10 にマッピングする例を示します。

```
Console> (enable) set security acl map IPACL1 10
ACL IPACL1 mapped to vlan 10
Console> (enable)
```

次に、コミットしていない ACL をマッピングしようとした場合の出力例を示します。

```
Console> (enable) set security acl map IPACL1 10
Commit ACL IPACL1 before mapping.
Console> (enable)
```

VACL の内容の表示

VACL の内容を表示するには、**show security acl info** コマンドを使用します。

VACL の内容を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL の内容を表示します。	**show security acl info** {*acl_name* | **all**} [**editbuffer** [*editbuffer_index*]]

次に、NVRAM に保存した VACL の内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL1
set security acl ip IPACL1
------------------------------------------------------------------
1. deny A
2. deny ip B any
3. deny c
4. permit any
```

次に、編集バッファ内にある VACL の内容を表示する例を示します。

```
Console> (enable) show security acl info IPACL1 editbuffer
set security acl ip IPACL1
-------------------------------------------------------------------
1. deny A
2. deny ip B any
3. deny C
4. deny D
5. permit any
Console> (enable)
```

VACL/VLAN のマッピングの表示

show security acl map コマンドを使用して、特定の ACL または VLAN の VACL/VLAN マッピングを表示することができます。

VACL/VLAN マッピングを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL/VLAN のマッピングを表示します。	**show security acl map** {*acl_name* | *vlan* | **all**}

次に、特定の VACL のマッピングを表示する例を示します。

```
Console> (enable) show security acl map IPACL1
ACL IPACL1 is mapped to VLANs:
1
Console> (enable)
```

次に、特定の VLAN のマッピングを表示する例を示します。

```
Console> (enable) show security acl map 1
VLAN 1 is mapped to IP ACL IPACL1.
VLAN 1 is mapped to IPX ACL IPXACL1.
VLAN 1 is mapped to MAC ACL MACACL1.
Console> (enable)
```

編集バッファの消去

rollback コマンドを使用して、最後に保存したあとに行った ACL 編集バッファの変更を消去することができます。ACL は、最後の **commit** コマンド実行時の内容に戻ります。

ACL 編集バッファの内容を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 編集バッファの内容を消去します。	**rollback security acl** {*acl_name* | **all** | **adjacency**}

次に、特定のセキュリティ ACL について、編集バッファの内容を消去する例を示します。

```
Console> (enable) rollback security acl IPACL1
Editbuffer for 'IPACL1' rolled back to last commit state.
Console> (enable)
```

セキュリティ ACL からの ACE の削除

ACL から特定の ACE またはすべての ACE を削除するには、**clear security acl** コマンドを使用します。このコマンドは、編集バッファから ACE を削除します。

セキュリティ ACL から ACE を削除するには、イネーブル モードで次の作業を行います。

作業	コマンド
セキュリティ ACL から ACE を削除します。	**clear security acl all** **clear security acl** *acl_name* **clear security acl** *acl_name editbuffer_index*

次に、すべての ACL から ACE を削除する例を示します。

```
Console> (enable) clear security acl all
All editbuffers modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、特定の ACL から特定の ACE を削除する例を示します。

```
Console> (enable) clear security acl IPACL1 2
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

セキュリティ ACL マップの消去

VACL/VLAN マッピングを削除するには、**clear security acl map** コマンドを使用します。

セキュリティ ACL マップを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
セキュリティ ACL マップを消去します。	**clear security acl map all** **clear security acl map** *acl_name* **clear security acl map** *vlan* **clear security acl map** *acl_name vlan*

次に、すべての VACL/VLAN マッピングを消去する例を示します。

```
Console> (enable) clear security acl map all
Map deletion in progress.

Successfully cleared mapping between ACL ip1 and VLAN 10.

Successfully cleared mapping between ACL ipx1 and VLAN 10.

(テキスト出力は省略)
Console> (enable)
```

次に、特定の VLAN 上の特定の VACL のマッピングを消去する例を示します。

```
Console> (enable) clear security acl map IPACL1 50
Map deletion in progress.

Successfully cleared mapping between ACL ipacl1 and VLAN 50.
Console> (enable)
```

VACL 管理情報の表示

VACL 管理情報を表示するには、**show security acl resource-usage** コマンドを使用します。

VACL 管理情報を表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
VACL 管理情報を表示します。	**show security acl resource-usage**

次に、VACL 管理情報を表示する例を示します。

```
Console> (enable) show security acl resource-usage
ACL resource usage:
ACL storage (mask/value): 0.29%/0.10%
ACL to switch interface mapping table: 0.39%
ACL layer 4 port operators: 0.0%
Console (enable)
```

特定ポート上でのトラフィック フローのキャプチャ

set security acl（**ip**、**ipx**、および **mac**）コマンドの **capture** キーワードを入力して、指定したフローと一致するパケットをキャプチャして、キャプチャ ポートから送出することができます。キャプチャ ポートは、**set security acl capture-ports** *mod/ports...* コマンドを使用して指定します。**capture** キーワードを使用すると、指定したフローと一致するパケットが、通常どおりスイッチングされるほか、キャプチャされ、キャプチャ ポートから送出されます。キャプチャ ポートはキャプチャしたすべてのトラフィックを送出するわけではありません。キャプチャ ポートの VLAN に属するトラフィックだけを送出します。

設定時の注意事項

ここでは、キャプチャ ポート設定時の注意事項について説明します。

- キャプチャ ポートは、EtherChannel の一部にすることはできません。
- キャプチャ ポートは、ATM（非同期転送モード）ポートとして使用することはできません。
- キャプチャ ポートは、VLAN のスパニングツリー フォワーディング ステートに設定する必要があります。
- 任意の数のスイッチ ポートをキャプチャ ポートとして指定することができます。キャプチャ ポートは、キャプチャ ポート リストに追加され、その設定が NVRAM に保存されます。
- 許可トラフィックだけがキャプチャされます。ACL により廃棄されたパケットはキャプチャできません。
- キャプチャ ポートは、キャプチャしたすべてのトラフィックを送出するわけではありません。キャプチャ ポートの VLAN に属するトラフィックだけが送出されます。多数の VLAN に宛てられたトラフィックをキャプチャするには、キャプチャ ポートを、必要な VLAN をサポートするトランクとして設定する必要があります。

  ルーテッド トラフィックの場合、キャプチャ ポートがパケットを送信するのは、レイヤ 3 でスイッチングされたあとだけです。したがって、レイヤ 3 でスイッチングされたフローの出力 VLAN がキャプチャ ポートの VLAN と一致する場合に限り、パケットがポートから送出されます。たとえば、VLAN 10 から VLAN 20 へのフローがある場合、（VLAN の 1 つに）これらのフローを許可する VACL を追加し、キャプチャ ポートを指定したと想定します。この場合、トラフィックがキャプチャ ポートから送出されるのは、トラフィックが VLAN 20 に属しているか、またはポートが VLAN 20 をサポートするトランクの場合だけです。キャプチャ ポートが VLAN 10 に存在する場合は、トラフィックは送出されません。キャプチャ ポートがトラフィックを送出するかどうかは、VACL が設定されている VLAN とは無関係です。

  1 つの VLAN から多数の VLAN に宛てられるトラフィックをキャプチャしたい場合には、キャプチャ ポートを、すべての出力 VLAN をサポートするトランクとして設定する必要があります。

  ブリッジド トラフィックの場合、すべてのトラフィックは同じ VLAN 内にとどまるため、キャプチャ ポートはブリッジド トラフィックと同じ VLAN 内に存在します。
- トラフィックをキャプチャするには、1 つの ACL を設定して VLAN グループにマッピングするか、複数の ACL を設定して各 ACL を 1 つの VLAN にマッピングします。必要なトラフィックをキャプチャするには、1 つの ACL ごとに必要なだけ ACE を設定します。

トラフィック フローをキャプチャする手順は、次のとおりです。

（注）　この説明では IP VACL を使用していますが、同じ手順で IPX および non-IP version 4/non-IPX VACL を設定することもできます。

ステップ 1　**set security acl ip** コマンドを入力して VACL を作成し、ACE を追加します。**capture** キーワードを指定します。

ステップ 2　**commit** コマンドを入力して、VACL および関連付けられた ACE を NVRAM にコミットします。

ステップ 3　**set security acl map** コマンドを入力して、VACL を VLAN にマッピングします。

ステップ 4　**set security acl capture-ports** *mod/ports...* コマンドを入力して、キャプチャ ポートを指定します。

設定例

次に、my_cap に 1 つの ACE を作成し、許可トラフィックをキャプチャするように指定する例を示します。

```
Console> (enable) set security acl ip my_cap permit ip host 60.1.1.1 host 60.1.1.98
capture
my_cap editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、my_cap ACL を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl my_cap
ACL commit in progress.

ACL my_cap successfully committed.
Console> (enable)
```

次に、my_cap を VLAN 10 にマッピングする例を示します。

```
Console> (enable) set security acl map my_cap 10
Mapping in progress.

VLAN 10 successfully mapped to ACL my_cap.
The old mapping with ACL captest was replaced with the new one.
Console> (enable)
```

次に、キャプチャ ポートを指定する例を示します。

```
Console> (enable) set security acl capture-ports 1/1-2,2/1-2
Successfully set the following ports to capture ACL traffic:
1/1-2,2/1-2
Console> (enable)
```

次に、キャプチャ ポートとして指定したポートを表示する例を示します。

```
Console> (enable) show security acl capture-ports
ACL Capture Ports: 1/1-2,2/1-2
Console> (enable)
```

次に、キャプチャ ポートを削除する例を示します。

```
Console> (enable) clear security acl capture-ports 1/1,2/1
Successfully cleared the following ports:
1/1,2/1
Console> (enable)
```

次に、ポート 1/1 および 2/1 が削除された例を示します。

```
Console> (enable) show security acl capture-ports
ACL Capture Ports:1/2,2/2
Console> (enable)
```

VACL ロギングの設定

（注）　この機能を使用できるのは、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 だけです。

拒否 VACL に対して **log** キーワードを使用すると、標準 IP アクセス リストについて、拒否されたパケットのメッセージを記録できます。アクセス リストに一致するパケットによって、コンソールに送信されるパケットに関する情報ロギング メッセージが生成されます。コンソールに記録されるメッセージのレベルは、**set logging level acl** *severity* コマンドによって制御されます。

最初のパケットはアクセス リストをトリガし、それによってただちにロギング メッセージが生成されます。それ以降のパケットは、5 分間隔で収集されてから、表示または記録されます。ロギング メッセージには、過去 5 分間に受信したパケットのフロー パターンと数が含まれています。

デフォルトでは、システム ロギング メッセージがコンソールに送信されます。Syslog サーバにシステム ロギング メッセージを送信するように、スイッチを設定することができます。システム メッセージ ロギングの設定については、第 28 章「システム メッセージ ロギングの設定」を参照してください。

設定時の注意事項

ここでは、VACL ロギング設定時の注意事項について説明します。

- IP VACL からの拒否トラフィックのみを記録します。
- ロギング レベルは 6（情報）または 7（デバッグ）に設定します。

VACL のロギングをイネーブルにする手順は、次のとおりです。

ステップ 1　**set logging level acl** *severity* コマンドを入力して、ロギング レベルを 6（情報）または 7（デバッグ）に設定します。

ステップ 2　（任意）**set security acl log maxflow** *max_number* コマンドを入力して、最大フロー パターン数に基づいて新しいログ テーブルを割り当て、記録されたパケット情報を保存します。正常に実行されると、新しいバッファが古いものと置き換えられ、古いテーブルのフローがすべて消去されます。メモリが不足しているか、最大数が限度を超えている場合は、エラー メッセージが表示され、コマンドは廃棄されます。有効な値は、256 ～ 2048 で、デフォルト値は 500 です。

（注）　最大フロー パターンが max_num の限度を超えている場合は、エラー メッセージが表示され、コマンドは廃棄されます。このようなパケットのメッセージは記録されません。

ステップ 3　（任意）**set security acl log ratelimit** *pps* コマンドを入力して、pps（パケット / 秒）単位でリダイレクト レートを設定します。設定が範囲を超える場合は、コマンドは廃棄され、範囲がコンソールに表示されます。有効な値は 500 ～ 5000 で、デフォルト値は 2500 です。レート制限をディセーブルにするには、値を 0 に設定します。

（注）　リダイレクト レートが pps の範囲を超える場合は、コマンドは廃棄され、範囲がコンソールに表示されます。このようなパケットのメッセージは記録されません。

ステップ 4　**set security acl ip** *acl_name* **deny log** コマンドを入力して IP VACL を作成し、ロギングをイネーブルにします。

ステップ 5　**commit security acl** *acl_name* コマンドを入力して、VACL を NVRAM にコミットします。

ステップ 6　**set security acl map** *acl_name vlan* コマンドを入力して、VACL を VLAN にマッピングします。

設定例

次に、ロギング レベルを設定する例を示します。

```
Console> (enable) set logging level acl 6
System logging facility <acl> for this session set to severity 6(information)
```

次に、最大フローに基づく新しいログ テーブルを割り当てる例を示します。

```
Console> (enable) set security acl log maxflow 512
Set VACL Log table to 512 flow patterns.
```

次に、リダイレクト レートを設定する例を示します。

```
Console> (enable) set security acl log ratelimit 1000
Max logging eligible packet rate set to 1000pps.
```

次に、VACL ログの設定を表示する例を示します。

```
Console> (enable) show security acl log config
VACL LOG Configration
------------------------------------------------------------
Max Flow Pattern    : 512
Max Logging Eligible rate (pps) : 1000
```

次に、my_cap に ACE を 1 つ作成し、拒否されたトラフィックを記録するように指定する例を示します。

```
Console> (enable) set security acl ip my_cap deny ip host 21.0.0.1 log
my_cap editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、my_cap ACL を NVRAM にコミットする例を示します。

```
Console> (enable) commit security acl my_cap
ACL commit in progress.

ACL my_cap successfully committed.
Console> (enable)
```

次に、VACL を VLAN にマッピングする例を示します。

```
Console> (enable) set security acl map my_cap 1
Mapping in progress.
ACL my_cap successfully mapped to VLAN 1.
:
:
2000 Jul 19 01:14:06 %ACL-6-VACLLOG:VLAN 1(Port 2/1) denied ip tcp 21.0.0.1(2000) ->
255.255.255.255(3000), 1 packet
2000 Jul 19 01:19:06 %ACL-6-VACLLOG:VLAN 1(Port 2/1) denied ip tcp 21.0.0.1(2000) ->
255.255.255.255(3000), 7 packets
2000 Jul 19 01:25:06 %ACL-6-VACLLOG:VLAN 1(Port 2/2) denied ip tcp 21.0.0.1(2000) ->
255.255.255.255(3000), 1 packets
```

次に、ログ テーブルのフロー情報を表示する例を示します。

```
Console> (enable) show security acl log flow ip any any
Total matched entry number = 1
Entry No. #1, IP Packet
----------------------------------------
Vlan Number            : 1
Mod/Port Number        : 2/1
Source IP address      : 21.0.0.1
Destination IP address : 255.255.255.255
TCP Source port        : 2000
TCP Destination port   : 3000
Received Packet Number : 10
```

次に、ログ テーブルを消去する例を示します。

```
Console> (enable) clear security acl log flow
Log table is cleared.
Console> (enable)
```

すべてのパケット タイプに関する MAC ベース ACL 検索の設定

（注）　この機能を使用できるのは、PFC3B および PFC3BXL だけです。

ここでは、すべてのパケット タイプに関する MAC ベース ACL 検索の設定手順について説明します。

MAC ベース ACL の概要

PFC3A は IP と MAC の 2 つの ACL プロトコル タイプをサポートします。IP ACL は IP バージョン 4 パケットとのみ一致し、MAC ACL は PFC3A で*サポートされない*すべてのパケット タイプと一致します（詳細については、「non-IP version 4/non-IPX VACL（MAC VACL）の作成および ACE の追加」[p.15-53] を参照）。PFC3A でサポートされているパケット タイプは、IP バージョン 4、MPLS、ARP/RARP、および IP バージョン 6 です。ただし、Release 8.4(1) 以前のソフトウェア リリースで作成できるのは、IP バージョン 4 ACL のみです。サポートされないパケット タイプ（IPX パケット タイプなど）は、MAC ACL を使用して一致させます。

（注）　IPX パケット タイプは PFC および PFC2 でサポートされています。

すべてのパケット タイプに関する MAC ベース ACL 検索の使用

PFC3B および PFC3BXL では、MAC ACL を使用して、すべてのパケット タイプに関する ACL 検索を実行できます。この機能は、パケットが IP バージョン 4、IP バージョン 6、IPX、MPLS などのいずれであるかに関係なく、すべてのパケットに関して MAC ベース マッチングを実行する場合に便利です。この機能を利用すると、集約ポリサーと match-all MAC ACL を組み合わせて、VLAN に入るすべてのトラフィックを特定のレートに制限できます。

この機能は入力 VLAN 単位でイネーブルにされ、セキュリティ ACL（VACL）および QoS ACL に影響します。着信 VLAN でこの機能がイネーブルにされている場合、この VLAN に着信するすべてのパケットは、IP バージョン 4 パケットなどの場合であっても、MAC ベース ACL とマッチングされます。

MAC ACL では、IP バージョン 4 Ethertype が追加されるように *ethertype* オプションが拡張されていて、IP バージョン 4 パケットを特に対象とするように ACE を設定できます。

MAC ベース ACL への VLAN および CoS の追加

PFC3B および PFC3BXL では、ポート VLAN 検索をサポートする MAC ACL 検索キーの一部として、Class of Service（CoS; サービス クラス）および VLAN を追加できます。この機能は、VLAN を個別に処理できるトランク ポートで使用すると便利です。この拡張機能は、VACL および QoS MAC ACL に影響します。PFC3B および PFC3BXL では、MAC 検索キーのフレーム タイプ フィールドによって VLAN フィールドが過負荷になります。CoS および VLAN フィールドはマスク可能であるため、両方のフィールドをオプション パラメータとして追加し、古い MAC ACL 設定をサポートできます。

VLAN マッチング

PFC3B および PFC3BXL では、MAC ACL が入力にマッピングされている場合、パケットの入力 VLAN が MAC ACL とのマッチングに使用されます。同様に、MAC ACL が出力にマッピングされている場合、パケットに関連する出力 VLAN が MAC ACL とのマッチングに使用されます。

（注）　MAC ACL と VLAN マッチングは、ポートにのみ適用できます。

VLAN マッチングは MAC ベース ACL 検索機能と組み合わせて使用したり、独立して使用することができます。また、検索はポート VLAN 単位で実行できます（VLAN 範囲全体がサポートされます）。

CoS マッチング

入力と出力のいずれの場合も、パケットに対応付けられた入力 CoS が MAC ACL とのマッチングに使用されます。入力 CoS は DBus ヘッダー内の CoS であり、ポートの信頼状態（trust-CoS/DSCP/IPprec/untrusted）、デフォルト CoS、および 802.1Q 対応ポートの CoS/CoS マッピング テーブルを問い合わせたあとに構築されます。

（注）　CoS マッチング動作は、パケット転送方法に応じて、出力 ACL（VACL および QoS ACL）ごとに異なる場合があります。標準のハードウェア ショートカット パケットでは、出力 ACL は入力 ACL と同じ CoS に関してマッチングを行います。ただし、ルータやマルチキャスト読み取り / 書き込みエンジンなどの中間転送エンティティを介してパケットが転送される場合、DBus CoS は通常、入力 DBus CoS と異なります。

CoS マッチングは MAC ベース ACL 検索機能と組み合わせて使用したり、または独立して使用することができます。

設定時の注意事項

MAC ベース ACL 検索を設定する場合は、次の注意事項に従ってください。

- この機能をイネーブルにする必要があるのは、レイヤ 2 VLAN のみです（この推奨事項は Metro カスタマーに適用されます）。
- レイヤ 3 VLAN 上でこの機能をイネーブルにする場合は、次の点に注意してください。
  - 一部のレイヤ 3 機能が失われ、次の警告メッセージが表示されます。

    ```
    Warning:IP RACLs, VACLs & some IP features will be ineffective on these vlans.
    ```

- パケットがハードウェア転送されるか、またはソフトウェア転送されるかに応じて、出力 ACL 検索に矛盾が生じることがあります。この機能をすべての VLAN でイネーブルにして、矛盾を回避することを推奨します（この推奨事項は Enterprise カスタマーに適用されます）。

すべてのパケット タイプに関する MAC ベース ACL 検索の設定

ここに記載されたコマンドは、VACL および QoS MAC ACL の両方に影響します。**set acl mac-packet-classify** *vlans* コマンドを使用すると、送信元 VLAN に着信したすべてのパケット タイプに関して MAC 検索をイネーブルにできます。**clear acl mac-packet-classify** [*vlans*] コマンドを使用すると、指定された VLAN の設定をデフォルトに戻します。デフォルト動作では、MAC ACL に一致するのは MAC パケットのみです。**clear acl mac-packet-classify** [*vlans*] コマンドを使用して VLAN を指定しない場合は、すべての VLAN でこの機能がディセーブルになります。**show acl mac-packet-classify** コマンドを使用すると、MAC パケット分類機能がイネーブルになっている VLAN リストが表示されます。

MAC ACL および拡張 Ethertype への CoS、VLAN、およびパケット タイプの追加

VACL および QoS ACL CLI は、CoS および VLAN に関するマッチングのオプション パラメータを追加するように、拡張されています。これらのコマンドは、次のとおりです。

```
Usage: set security acl mac {acl_name} {permit | deny}
            <src_mac_addr_spec> <dest_mac_addr_spec>
            [<ethertype>] [capture]
            [cos <cos_value>]
            [vlan <vlan>]
            [before <editbuffer_index>|modify <editbuffer_index>]
            (mac_addr_spec = <addr> <mask> or host <addr> or any
     example: 11-22-33-44-00-00 00-00-00-00-ff-ff, host 11-22-33-44-55-66)
            ethertype = names or 0x0, 0x05ff - 0xffff,
            cos_value = 0..7, vlan = 1..4094,

Usage: set qos acl mac {acl_name} {dscp dscp | trust-cos}
            [aggregate <aggregate_name>]
            <src_mac_addr_spec> <dest_mac_addr_spec> [<ethertype>]
            [cos <cos_value>]
            [vlan <vlan>]
            [before <editbuffer_index>|modify <editbuffer_index>]
            (mac_addr_spec = <addr> <mask> or host <addr> or any
     example: 11-22-33-44-00-00 00-00-00-00-ff-ff, host 11-22-33-44-55-66)
            ethertype = names or 0x0, 0x05ff - 0xffff,
            cos_value = 0..7, vlan = 1..4094,
```

CoS および VLAN フィールドはオプションです。このフィールドを指定しない場合は、すべての CoS または VLAN 値と一致します。

（注）VLAN マッチ オプションが指定された ACL は、ポートにのみマッピングできます。

（注）**set acl mac-packet-classify** *vlans* コマンドを使用すると、すべての Cisco IOS ACL が操作不能になります。

IP バージョン 4 オプションを追加するように、Ethertype が拡張されています。これにより、MAC ACL 検索を使用する場合に、IP バージョン 4 パケットを特に対象とすることができます。IP バージョン 4 オプションを選択した場合は、**set acl mac-packet-classify** *vlans* コマンドを使用して、対応する VLAN がイネーブルにされているか確認する必要があります。次のように、IP バージョン 4 オプションが追加されました。

```
Console> (enable) set security acl mac macacl1 permit any any ?
  <0x0, 0x0600 - 0xffff>     Match an EtherType value
  ipv4                       (0x8000)
  ipx-arpa                   (0x8137) Use 0xffff to match on non-arpa IPX
  .......
Console> (enable)
```

次に、MAC ベース ACL 検索 CLI の例を示します。

```
Console> (enable) set acl mac-packet-classify 5
Enabled mac-packet-classify on vlan(s) 5.
Warning:IP RACLs, VACLs & some IP features will be ineffective on these vlans.
Console> (enable) show acl mac-packet-classify
Feature enabled on source vlan(s) 1,5.
Console> (enable) clear acl mac-packet-classify 5
Disabled mac-packet-classify on vlan(s) 5.
Console> (enable)
```

（注）　**set** および **clear** コマンドに **all** キーワードを使用すると、すべての VLAN を指定できます。

VACL および QoS ACL の設定およびフラッシュ メモリへの保存

ここでは、VACL および QoS ACL を設定し、NVRAM ではなくフラッシュ メモリに保存する手順について説明します。これまでの作業では、設定情報はすべて NVRAM に保存されます。QoS およびセキュリティ ACL（VACL）を追加すると、NVRAM の空き容量がなくなることがあります。NVRAM の空き容量がなくなると、ACL 設定が制限されるほか、ソフトウェア バージョンのアップグレード時にも支障があります。

（注）　ほとんどの場合、VACL および QoS ACL を保存するには 512 KB の NVRAM で十分です。そのため、デフォルトでは、すべての ACL 設定が NVRAM に保存されます。

ここで説明する作業は、次のとおりです。

- VACL および QoS ACL 設定のフラッシュ メモリへの自動的な移動（p.15-67）
- VACL および QoS ACL 設定のフラッシュ メモリへの手動での移動（p.15-68）
- VACL および QoS ACL 設定のフラッシュ メモリからの実行（p.15-70）
- VACL および QoS ACL 設定の NVRAM への再移動（p.15-70）
- 冗長構成の同期化サポート（p.15-70）
- ハイ アベイラビリティの保証（p.15-70）

（注）　ここで使用するコマンドの詳細については、第 24 章「スイッチの起動設定の変更」を参照してください。

VACL および QoS ACL 設定のフラッシュ メモリへの自動的な移動

VACL および QoS ACL 設定がフラッシュ メモリに自動的に移動するのは、システム ソフトウェアのアップグレード時に、アップグレードに必要な NVRAM 容量が不足している場合だけです。ソフトウェア アップグレードの実行に必要な NVRAM 容量が不足している場合、NVRAM から QoS ACL および VACL の設定が削除され、ACL 設定が自動的にフラッシュ メモリに移されます。この場合、次の Syslog メッセージが表示されます。

```
1999 Sep 01 17:00:00 %SYS-1-CFG_FLASH:ACL configuration moved to
bootflash:switchapp.cfg
1999 Sep 01 17:00:00 %SYS-1-CFG_ACL_DEALLOC:NVRAM full. Qos/Security ACL configuration
deleted from NVRAM.
```

これで、VACL および QoS ACL 設定がフラッシュ メモリに正常に移動したことが確認できます。この間システムは、同時に次の処理も実行します。

- CONFIG_FILE 変数を bootflash:switchapp.cfg に設定します。
- **set boot config-register auto-config** コマンドの **recurring**、**append**、および **sync** オプションをイネーブルにします。

アップグレード中にエラーが発生すると、次の Syslog メッセージが表示されます。

```
1999 Sep 01 17:00:00 %SYS-1-CFG_FLASH_ERR:Failed to write ACL configuration to
bootflash:switchapp.cfg
1999 Sep 01 17:00:00 %SYS-1-CFG_ACL_DEALLOC:NVRAM full. Qos/Security ACL configuration
deleted from NVRAM.
```

これらのエラー メッセージが表示された場合、VACL および QoS ACL 設定は DRAM だけに保存されています。フラッシュ メモリ内に空き容量を確保して設定をフラッシュ メモリに保存する必要があります（「VACL および QoS ACL 設定の NVRAM への再移動」[p.15-70] を参照）。または、不要な VACL および QoS ACL を削除して、**set config acl nvram** コマンドで ACL 設定を NVRAM に保存することもできます。

VACL および QoS ACL 設定のフラッシュ メモリへの手動での移動

VACL および QoS ACL 設定が、512 KB の NVRAM 容量を超える場合には、次の手順で、VACL および QoS ACL の設定を手動でフラッシュ メモリに移動することができます。

ステップ 1　起動時のスイッチ設定に使用する VACL および QoS ACL auto-config ファイルを指定します。

```
Console> (enable) set boot auto-config bootflash:switchapp.cfg
CONFIG_FILE variable = bootflash:switchapp.cfg
Console> (enable)
```

ステップ 2　スイッチのリセットまたはいったん電源を切ってから再投入する際に、CONFIG_FILE 環境変数の値を保持する（**recurring** キーワード）かまたは消去する（**non-recurring** キーワード）かを指定します。

```
Console> (enable) set boot config-register auto-config recurring
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, overwrite, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

ステップ 3　auto-config ファイルにより、NVRAM の設定を上書きするか、または現在の NVRAM の内容に追加するかを指定します。

```
Console> (enable) set boot config-register auto-config append
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, append, sync disabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

ステップ 4　同期化をイネーブルにするか、ディセーブルにするかを指定します。同期化をイネーブルにすると、auto-config ファイルにより、スタンバイ スーパバイザ エンジンが自動的に同期化されます。

```
Console> (enable) set boot config-register auto-config sync enable
Configuration register is 0x12F
ignore-config: disabled
auto-config: recurring, append, sync enabled
console baud: 9600
boot: image specified by the boot system commands
Console> (enable)
```

ステップ 5　コミットした VACL および QoS ACL 設定の変更を、auto-config ファイルに保存します。

```
Console> (enable) copy acl-config bootflash:switchapp.cfg
Upload ACL configuration to bootflash:switchapp.cfg
2843644 bytes available on device bootflash, proceed (y/n) [n]? y
ACL configuration has been copied successfully.
Console> (enable)
```

ステップ 6　NVRAM から、VACL および QoS ACL の設定を削除します。

```
Console> (enable) clear config acl nvram
ACL configuration has been deleted from NVRAM.
Warning: Use the copy commands to save the ACL configuration to a file and
the 'set boot config-register auto-config' commands to configure the
auto-config feature.
```

（注）　auto-config ファイルには、VACL および QoS ACL のマッピング コマンド（**set qos acl map** および **set security acl map**）も保存されます。VACL および QoS ACL の設定をフラッシュ メモリに保存するとき、マッピング コマンドを使用している場合には、**copy** コマンドを使用して設定をフラッシュ メモリに保存する必要があります。

この時点で VACL および QoS ACL 設定は、NVRAM から削除されています。設定は auto-config ファイルの bootflash:switchapp.cfg に保存されており、システムの起動時に NVRAM 設定に付加されます。

VACL および QoS ACL 設定に変更を加え、変更をコミットした場合には、**copy acl-config bootflash:switchapp.cfg** コマンドを使用して、設定を auto-config ファイルに保存する必要があります。

同期化をイネーブルに設定したので、auto-config ファイルの内容はスタンバイ スーパバイザ エンジンに自動的に反映されます。

VACL および QoS ACL 設定をフラッシュ メモリに書き込めない場合、設定は NVRAM から削除されています。その場合、VACL および QoS ACL 設定が保存されている場所は DRAM のみになります。システムをリセットすると、VACL および QoS ACL 設定はデフォルト設定に戻ります。

（注）　設定をフラッシュ メモリに書き込めない場合には、設定をファイルにコピーし、フラッシュ メモリの空き容量を増やしてから、VACL および QoS ACL 設定を再びフラッシュ メモリに書き込んでください。

システムの起動時に、VACL および QoS ACL 設定の保存場所がフラッシュ メモリに設定されている場合、CONFIG_FILE 変数が設定されていないか、指定したファイルが存在しないと、次の Syslog メッセージが表示されます。

```
1999 Sep 01 17:00:00 %SYS-0-CFG_FLASH_ERR:ACL configuration set to flash but no ACL
configuration file found.
```

VACL および QoS ACL 設定のフラッシュ メモリからの実行

VACL および QoS ACL 設定をフラッシュ メモリに移動したあとは、QoS ACL および VACL のコミット動作は NVRAM に書き込まれません。次のように、設定を手動でフラッシュ ファイルにコピーする必要があります。

- **set boot config-register auto-config append** オプションを使用すると、auto-config ファイルの設定が NVRAM 設定に追加されます。コミットしたあと、VACL および QoS ACL の設定をこのファイルにコピーするだけで済みます。
- **set boot config-register auto-config append** オプションを使用しないと、システムの起動時に、NVRAM の設定が消去されてから、auto-config ファイルが実行されます。この場合、NVRAM に保存した変更は失われます。保存する場合には、（VACL および QoS ACL 設定だけでなく）設定全体を auto-config ファイルにコピーしておく必要があります。

VACL および QoS ACL 設定の NVRAM への再移動

次に、VACL および QoS ACL の設定を NVRAM に戻す例を示します。

```
Console> (enable) set config acl nvram
ACL configuration copied to NVRAM.
Console> (enable)

Console> (enable) clear boot auto-config
CONFIG_FILE variable =
Console> (enable)
```

冗長構成の同期化サポート

set boot コマンドには、auto-config ファイルを自動的に同期化するオプションがあります。

auto-config オプションをイネーブルにして、VACL と QoS ACL の設定がフラッシュ メモリにある場合、アクティブ スーパバイザ エンジン上の auto-config ファイルの変更は常に、スタンバイ スーパバイザ エンジンに同期化されます。たとえば、アクティブ スーパバイザ エンジン上の auto-config ファイルを削除すると、スタンバイ スーパバイザ エンジン上でもそのファイルが削除されます。同様に、新しいスタンバイ スーパバイザ エンジンを搭載すると、アクティブ スーパバイザ エンジンにより、auto-config ファイルが自動的に同期化されます。

ハイ アベイラビリティの保証

スーパバイザ エンジンがスイッチオーバーしても、スタンバイ スーパバイザ エンジンの VACL および QoS ACL 設定は、アクティブ スーパバイザ エンジンの内容、すなわち NVRAM に保存されている VACL および QoS ACL 設定とまったく同じです。唯一の違いは、スタンバイ スーパバイザ エンジンではデータは DRAM に保存されますが、スイッチオーバーの機能的な動作の変更がないことです。

ポート単位の ACL の設定

（注）　この機能を使用できるのは、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720 および PFC3B/PFC3BXL 搭載の Supervisor Engine 32 のみです。

ここでは、Port ACL（PACL; ポート ACL）について説明します。

PACL 設定の概要

Release 8.3(1) より前のソフトウェア リリースでは、VACL および Cisco IOS ACL という 2 種類のアクセス リストのみがありました。VACL はレイヤ 2 およびレイヤ 3 転送トラフィックに適用されましたが、Cisco IOS ACL はレイヤ 3 転送パケットにのみ適用されました。いずれのタイプのアクセス リストも VLAN に適用され、パケット ヘッダー情報に基づいてトラフィックをフィルタリングしていました。

Release 8.3(1) には、PACL という追加のアクセス リスト タイプがあります。PACL は、物理ポートにマッピングされるアクセス リストです（通常、VLAN は複数の物理ポートで構成されます）。PACL では、さらに粒度を上げて特定の物理ポート上のトラフィックをフィルタリングします。VACL と同様に、PACL はレイヤ 2 およびレイヤ 3 転送パケットに適用されます。

図 15-9 に、アクセス リストのタイプ間の論理関係を示します。PACL は、まず物理ポートの着信パケットに適用されます。パケットが PACL によって許可されると、関連する入力 VLAN に適用されている VACL によってフィルタリングされます。パケットがレイヤ 3 で転送されて VACL によって許可される場合、同じ VLAN の Cisco IOS ACL でフィルタリングされます。出力方向については、同じ処理が逆方向で行われます。ただし、現在出力 PACL についてはハードウェアのサポートがありません。

図 15-9　アクセス リストのタイプ間の論理関係

PACL には、ポート単位で設定可能な 3 種類の操作モードがあります。

- ポートベース — PACL が既存の VACL および Cisco IOS ACL を上書きします。このモードでは、Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）および NAT などの機能は、物理ポートで機能しません。
- VLAN ベース — VACL および Cisco IOS ACL が PACL を上書きします。
- マージ — このモードでは、入力PACL、VACL、および Cisco IOS ACL が、図 15-9 に示す論理シリアル モデルでマージされます。

ACL がポートにマッピングされていない場合、ポートは内部で VLAN ベース モードに戻ります。

ポートがマージ モードである場合を除き、PACL をトランキング ポートに設定できます。トランキング ポートが独自の ACL を持つ複数の VLAN を設定できるために、このような制限があります。VLAN x 用の VACL を、VLAN y がタグ付けされたパケットに適用する方法は誤りです。PFC3A はポート /VLAN ペアに基づいて検索ができないため、マージ モードで PACL をポートにマッピングできません。

（注）　PACL を作成するための CLI 構文は、VACL のものと同じです。ポートにマッピングされた ACL のインスタンスを PACL といいます。VLAN にマッピングされた ACL のインスタンスを VACL といいます。同じ ACL をポートと VLAN の両方にマッピングできます。VACL と同様に、PACL はすべてのプロトコル タイプでサポートされます。

PACL 設定時の注意事項

ここでは、PACL の設定時の注意事項について説明します。

PACL の VACL および Cisco IOS ACL との相互作用

ここでは、PACL の VACL および Cisco IOS ACL との相互作用における注意事項について説明します。

- ポートがポートベース モードに設定されている場合に、PACL は VACL および Cisco IOS ACL の両方を上書きします。この規則の例外の 1 つとして、パケットが MSFC によってソフトウェアで転送される場合があります。パケットは、PACL モードに関係なく適用された入力 Cisco IOS ACL を取得します。パケットがソフトウェアで転送される例として、次の 2 つがあります。
  - （ロギングや NAT などの機能により）出力ブリッジングされたパケット
  - IP オプションが設定されているパケット

  MSFC は、検出されたパケットに入力および出力 Cisco IOS ACL を再適用します。レイヤ 3 ハードウェアおよびソフトウェア転送パケットに対する PACL 上書きモードは、Cisco IOS ACL とは異なります。
- PACL がキャプチャを許可するように設定されていて VACL が同じパケットを拒否するように設定されている場合、マージ結果は設定誤りとなります。このような場合、PACL が [merge disabled] 状態になります。

EtherChannel および PACL の相互作用

ここでは、EtherChannel および PACL の相互作用における注意事項について説明します。

- 異なる PACL 設定を持つポートは、ポート チャネルを形成できません。ポート チャネルを形成するには、ポートには同じ PACL モード（ポートベース、VLAN ベース、またはマージ）および同じ ACL 名がなければなりません。

- EtherChannel のポートをポートベース ACL から VLAN ベース ACL に変更した場合、そのチャネル内のすべてのポートが VLAN ベース ACL モードに変更されます。
- あるポートの設定変更は、チャネル内のすべてのポートに影響します。あるチャネルに属するポートに ACL をマッピングすると、チャネルに関連付けられた論理ポートを含むチャネル内のすべてのポートにもマッピングされます。すべての物理ポートへのマッピングは、ポートチャネルが破壊されたあとでもハードウェアおよび NVRAM 内に残ります。論理ポートへのマッピングのみが削除されます。
- 新しい PACL が EtherChannel 内のあるポートに適用された場合、チャネル内のすべてのポートが新しい ACL マップを使用するように設定されます。

ダイナミック ACL（マージ モードにのみ適用）

ダイナミック ACL は VLAN ベースで、CBAC および IGMP の 2 つの機能によって使用されます。マージ モードは、ダイナミック ACL と PACL とのマージを*サポートしません*。マージ モードでは、次のような設定はできません。

- 対応する VLAN にダイナミック ACL がマッピングされているポートに PACL を適用しようとすること。
- 構成ポートの 1 つに PACL がインストールされている VLAN にダイナミック ACL を適用しようとすること。ダイナミック ACL は正常にマッピングされますが、矛盾のあるポートが [merge disable] モードになります。ダイナミック ACL が削除されたあとにポートが再びアクティブになります。

トランキング モード（マージ モードにのみ適用）

マージ モードの PACL は、トランキング ポートと互換性がありません。ポートをマージ モードに設定するには、ポートのトランキング モードを **off** に設定する必要があります。逆に言うと、マージ モードのポートはトランキング モードに変更できません。

補助 VLAN（マージ モードにのみ適用）

補助 VLAN がイネーブルのポートにマージ モードを設定できません。逆に言うと、補助 VLAN がイネーブルのポートをマージ モードに変更できません。

プライベート VLAN（マージ モードにのみ適用）

VACL をプライマリまたはセカンダリ プライベート VLAN にマッピングできます。対照的に、Cisco IOS ACL はプライマリ VLAN にしかマッピングできません。プライマリ VLAN にマッピングされる入力 Cisco IOS ACL は、すべての対応するセカンダリ VLAN にマッピングされ、プライマリ VLAN にはマッピングされません。プライマリ VLAN にマッピングされる出力 Cisco IOS ACL は、プライマリ VLAN にマッピングされます。

プライベート VLAN の入力ルックアップは、セカンダリ VLAN でのみ実行されます。マージ モードでは、PACL はセカンダリ VLAN に適用されている入力 VACL および Cisco IOS ACL とマージされます。

ポート VLAN アソシエーション変更（マージ モードにのみ適用）

ポート VLAN アソシエーション変更は、すべての場合に適用されます。ただし、ポートがマージ モードに設定されている場合、ポート VLAN アソシエーションでの変更によりマージ障害が発生する場合があります。そのような場合、ポートは [merge disable] モードになります。

PACL のマッピングを解除したあとに再度マッピングするか、Cisco IOS ACL が自動的に再マージをトリガします。次に、ポート 3/1 が VLAN 1 に関連付けられたあとに VLAN 2 に関連付けられる例を示します。

```
Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
ACL ipacl1 is successfully mapped to port(s) 3/1.

Console> (enable) set security acl map ipacl2 1
ACL ipacl2 is successfully mapped to VLAN 1.

Console> (enable) set security acl map ipacl3 2
ACL ipacl3 is successfully mapped to VLAN 2.

Console> (enable) set vlan 2 3/1
2003 Sep 05 22:34:50 %ACL-3-PACLMERGEFAILED:Failed to merge Security ACLs on Port(s)
3/1 with Vlan 2.
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- -----------------------
2     3/1

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge      (VLAN=2) disabled



Config:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                             IP

Runtime:
Port  ACL name                          Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable) show security acl map runtime 1
Vlan ACL name                           Type
---- -------------------------------- ----
   1 ipacl2                              IP

Console> (enable) show security acl map runtime 2
Vlan ACL name                           Type
---- -------------------------------- ----
   2 ipacl3                              IP
Console> (enable)
```

OIR の概要

モジュールを取り外したりリセットしたりする場合、モジュールに添付されている PACL も（ハードウェアにプログラミングされている）実行コンフィギュレーションおよび（NVRAM に保存されている）NVRAM コンフィギュレーションから削除されます。コンフィギュレーションは NVRAM に保存されますが、表示されません。モジュールを挿入したりオンラインにした場合、コンフィギュレーションは NVRAM（またはテキスト コンフィギュレーション ファイル）から再び読み込まれて実行コンフィギュレーションに再マッピングされます。

ポートのイネーブルまたはディセーブルは、ポートがマージ モードである場合を除いて、ACL マッピングまたはセキュリティ ACL モードに影響しません。マージ モードでは、VLAN でディセーブルになったり VLAN から消去されたポートは、ポートに関連した VLAN が使用できなくなりポートでパケットの転送や他の VLAN とのマージができなくなるため、[merge disable] ステートになります。

CLI での PACL の設定

ここでは、Catalyst 6500 シリーズ スイッチ上で PACL を作成し、アクティブにする手順について説明します。

- PACL モードの指定（p.15-75）
- PACL 情報の表示（p.15-76）
- ポートまたは VLAN への ACL のマッピング（p.15-76）
- ACL マッピング情報の表示（p.15-77）
- EtherChannel の ACL 情報の表示（p.15-78）

PACL モードの指定

デフォルトの PACL モードは VLAN ベースであり、既存の VACL 設定はアクティブのままです。

PACL モードを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
PACL モードを指定します。	**set port security-acl** *mod/ports*..[**port-based** | **vlan-based** | **merge**]

次に、ポート 3/1 に PACL を指定する例を示します。

```
Console> (enable) set port security-acl 3/1 port-based
Warning: Vlan-based ACL features will be disabled on port(s) 3/1.
ACL interface is set to port-based mode for port(s) 3/1.

Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge mode for port(s) 3/1.

Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.
Console> (enable)
```

次に、トランク ポート（ポート 3/1）をマージ モードにしようとした場合の応答の例を示します。

```
Console> (enable) set port security-acl 3/1-4 merge
ACL interface cannot be in merge mode on multi-vlan access port 3/1.
ACL interface is set to merge mode for port(s) 3/2.
ACL interface is set to merge mode for port(s) 3/3.
ACL interface is set to merge mode for port(s) 3/4.
```

PACL 情報の表示

show port security-acl *mod/port* コマンドは、指定したポートの PACL 情報を表示します。Config フィールドでは、NVRAM に保存されているものが表示されます。Runtime フィールドでは、実際にハードウェアにプログラミングされたものが表示されます。また、次のようなマージ操作のステータスも表示されます。

- active — ポートに PACL が設定されており、VLAN と正常にマージされています。
- inactive — ポートに設定されている PACL はありません。
- disabled — ポートに PACL が設定されていますが、(いくつかの理由で) マージに失敗しました。

show port security-acl コマンドも、ポートがマージするように設定されている VLAN を表示します。

PACL 情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PACL 情報を表示します。	**show port security-acl** *mod/port*

次に、ポート 3/1 の PACL 情報を表示する例を示します。

```
Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1      port-based     port-based         not applicable

Config:
Port  ACL name                          Type
----- --------------------------------- ----
 3/1  ipacl1                            IP

Runtime:
Port  ACL name                          Type
----- --------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

ポートまたは VLAN への ACL のマッピング

ポートが VLAN ベース モードの場合でも ACL をポートにマッピングできます。このような場合、コンフィギュレーションは NVRAM にコミットされて、あとでポートがポートベース モードまたはマージ モードに変更される際に、ハードウェアに復元されます。この機能は QoS と似ています。

ACL の VLAN へのマッピングでは、次のような操作が実行されます。

1. ACL が VLAN にマッピングされます。
2. マージ モードであるすべての構成ポートとともにマージが自動的にトリガされます。

(1) が失敗した場合、操作が失敗して Syslog メッセージが生成されます。(2) の場合、VACL とのマージに失敗したポートに対して Syslog が生成されます。これらのポートは一時的に VLAN ベース モードになります。ポートがマージに失敗した場合、**show port security-acl** *mod/port* コマンドを通じて表示されるマージのステータスは [merge disabled] になります。[merge disabled] ステータスの例については、「PACL の設定例」(p.15-78) の「例 6」を参照してください。

ポートまたは VLAN に ACL をマッピングするには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートまたは VLAN に ACL をマッピングします。	**set security acl map** *acl_name* [*mod/ports* | *vlans*]

次に、ポート 3/1 に ACL をマッピングする例を示します。

```
Console> (enable) set security acl map ipacl1 3/1
Mapping in progress.
ACL ipacl1 is successfully mapped to port(s) 3/1.

Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Port 3/1 is set to vlan-based mode, config is saved in Nvram.
Config will be applied when the port is set to port-based/merge mode.
Console> (enable)
```

ACL マッピング情報の表示

show security acl map コマンドは、次のように、ポート マッピングを表示するように拡張されました。

- 設定およびランタイム マッピングを表示するために必須キーワード（**config** および **runtime**）が追加されました。
- 設定された VACL および PACL を表示するために、任意キーワード（**all-vlans** および **all-ports**）が追加されました。

ACL マッピング情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
ACL マッピング情報を表示します。	**show security acl map** [**config** | **runtime**] [*acl_name* | *mod_num*/*port_num* | *vlan* | **all** | **all-vlans** | **all-ports**]

次に、ACL マッピング情報を表示する例を示します。

```
Console> (enable) show security acl map config all
ACL Name                          Type Ports/Vlans
--------------------------------- ---- --------------
ipacl1                            IP   11
ipacl2                            IP   3/1

Console> (enable) show security acl map config all-ports
ACL Name                          Type Ports
--------------------------------- ---- --------------
ipacl2                            IP   3/1

Console> (enable) show security acl map runtime 3/1
Port  ACL name                          Type
----- --------------------------------- ----
3 / 1 ipacl1                            IP
Console> (enable)
```

EtherChannel の ACL 情報の表示

ポート チャネル上に PACL マッピングを表示するために、**show channel** コマンドが拡張されました。*type* に対して、*security-acl* を指定できます。

EtherChannel の ACL 情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
EtherChannel の ACL 情報を表示します。	**show port channel** [**all** | *mod*[/*port*]] {**info** [*type*]}

次に、EtherChannel の ACL 情報を表示する例を示します。

```
Console> (enable) show port channel 3/40 info security-acl
Port  ACL-Interface Type
----- ------------------
 3/37 port-based
 3/38 port-based

Port  ACL name                           Type
----- -------------------------------- ------
 3/37 ipacl1                             IP
 3/38 ipacl1                             IP
Console> (enable)
```

PACL の設定例

ここでは、PACL の設定例を紹介します。

例 1

次に、ポートが VLAN ベース モードの場合に ACL をポートにマッピングする例を示します。

```
Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Port 3/1 is set to vlan-based mode, config is saved in Nvram.
Config will be applied when the port is set to port-based/merge.

Console> (enable) show security acl map config 3/1
Port  ACL name                           Type
----- -------------------------------- ----
 3/1  ipacl1                             IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                           Type
----- -------------------------------- ----
No ACL mapped to port 3/1.

Console> (enable) set port security-acl 3/1 port-based
Warning: Vlan-based ACL features will be disabled on port(s) 3/1.
ACL interface is set to port-based mode for port(s) 3/1.

Console> (enable) show security acl map config 3/1
Port  ACL name                           Type
----- -------------------------------- ----
 3/1  ipacl1                             IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                           Type
----- -------------------------------- ----
 3/1  ipacl1                             IP
Console> (enable)
```

例 2

次に、ACL マッピング エラーによりセキュリティ ACL モードが変更された場合に障害が発生する例を示します。この例では、ACL が NVRAM にのみマッピングされてハードウェアにはマッピングされません。

```
Console> (enable) set port security-acl 3/1 vlan-based
ACL interface is set to vlan-based mode for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Port 3/1 is set to vlan-based mode, config is saved in Nvram.
Config will be applied when the port is set to port-based/merge.

Console> (enable) set port security-acl 3/1 port-based
Warning: Vlan-based ACL features will be disabled on port(s) 3/1.
ACL interface is set to port-based mode for port(s) 3/1
2003 Sep 05 22:34:50 %ACL-3-TCAMFULL:Acl engine TCAM table is full
2003 Sep 05 22:34:50 %ACL-3-PACLMAPCOMMITFAIL:Failed to Map Security ACL ipacl1 to
Port 3/1

Console> (enable) show security acl map config 3/1
Port  ACL name                          Type
----- ------------------------------- ----
 3/1  ipacl1                           IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                          Type
----- ------------------------------- ----
No ACL is mapped to port 3/1.


Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1      port-based     port-based         not applicable

Config:
Port  ACL name                          Type
----- ------------------------------- ----
 3/1  ipacl1                           IP

Runtime:
Port  ACL name                          Type
----- ------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

例 3

次に、ポートがマージ モードに設定されているものの ACL にマッピングされない例を示します。

```
Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge mode for port(s) 3/1.

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge      (VLAN 5) inactive

Config:
Port  ACL name                          Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.

Runtime:
Port  ACL name                          Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable) set security acl map ipacl1 3/1
ACL ipacl1 is successfully mapped to port(s) 3/1.

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge        (VLAN 5) active

Config:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                            IP

Runtime:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                            IP


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

例 4

次に、ACL をポートにマッピングする際に発生する障害の例を示します。この場合、設定は保存されません。

```
Console> (enable) set port security-acl 3/1 merge
ACL interface is set to merge for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
Mapping in progress.
2003 Oct 01 19:44:31 %ACL-3-PACLMAPCOMMITFAIL:Failed to Map Security ACL ipacl1 to
Port 3/15
Failed to attach ACL ipacl1 to port(s) 3/1.

Console> (enable) show security acl map config 3/1
Port  ACL name                          Type
----- ------------------------------- ----
No ACL is mapped to port 3/1.

Console> (enable) show security acl map runtime 3/1
Port  ACL name                          Type
----- ------------------------------- ----
No ACL is mapped to port 3/1.
Console> (enable)
```

例 5

次に、ポートベース モードからマージ モードに変更する際に障害が発生した場合に、モードを変更できない例を示します。

```
Console> (enable) set port security-acl 3/1 port-based
ACL interface is set to port-based for port(s) 3/1.

Console> (enable) set security acl map ipacl1 3/1
ACL ipacl1 is successfully mapped to port 3/1.

Console> (enable) show security acl map config 3/1
Port  ACL name                          Type
----- ------------------------------- ----
 3/1  ipacl1                            IP

Console> (enable) show security acl map runtime 3/1
Port  ACL name                          Type
----- ------------------------------- ----
 3/1  ipacl1                            IP

Console> (enable) set port security-acl 3/1 merge
Failed to set interface to merge mode for port(s) 3/1.
2003 Oct 01 19:53:01 %ACL-3-TCAMFULL:Acl engine TCAM table is full
Console> (enable)
```

例 6

次に、VACL とのマージに失敗したポートに対して Syslog が生成され、これらのポートが一時的に VLAN ベース モードになる例を示します。マージ ステータスは [merge disabled] です。

```
Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge        (VLAN=5) active

Config:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC

Runtime:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable) set security acl map ipacl2 5
ACL ipacl2 is successfully mapped to VLAN 5.
2003 Oct 01 20:01:04 %ACL-3-MERGEFAILED:Failed to merge Security ACLs on ports(s)
3/1-4 with VLAN 5
2003 Oct 01 20:01:04 %ACL-3-PACLSMERGEDFORVLAN:Merge completed for all ports on Vlan 5

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge      (VLAN=5) disabled
Config:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC

Runtime:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                            IP
 3/1  macacl1                           MAC


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

例 7

次に、例 6 の続きで、VACL または PACL をマッピングまたはマッピング解除して障害ステートから回復する例を示します。この例では、MAC PACL を切り離すことである種の Ternary CAM（TCAM）リソースを解除して、マージを継続できるようにします。Syslog は、マージが再びイネーブルになると生成されます。

```
Console> (enable) clear security acl map macacl1
Map deletion in progress.
Successfully cleared mapping between ACL macacl1 and port 3/1.
2003 Oct 01 20:01:04 %ACL-3-PACLMERGED:Merged Security ACLs on port(s) 3/1

Console> (enable) show port security-acl 3/1
Port  Interface Type Interface Type Interface Merge Status
      config         runtime        runtime
----- -------------- -------------- ----------------------
 3/1           merge          merge        (VLAN=5) active

Config:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                             IP

Runtime:
Port  ACL name                          Type
----- -------------------------------- ----
 3/1  ipacl1                             IP


dhcp-snooping:
Port     Trust     Source-Guard    Source-Guarded IP Addresses
----- -----------  ------------    ---------------------------
 3/1   untrusted      disabled

Console> (enable)
```

ACL 統計情報の設定

ここでは、ACL 統計情報を設定する手順について説明します。

- ACL 統計情報の概要（p.15-84）
- CLI からの ACL 統計情報の設定（p.15-84）

ACL 統計情報の概要

set security acl コマンド セットに **statistics** キーワードを指定すると、ACE または ACL（VACL および PACL）に関する統計情報が保存されます。ACL 統計情報はデフォルトでディセーブルです。ACL 単位、VLAN 単位、ACE 単位でイネーブルにできます。

ACL は TCAM でプログラミングされる前に、ACL コンパイラに渡されます。ACL コンパイラは ACL の ACE 数を最適化し、マスクをできるだけ共有することにより、使用される TCAM マスク数を削減します。インターフェイス上に ACL を介して設定された機能 / ポリシーが複数存在する場合は、これらの ACL がマージされ、マージされた ACL が最適化されます。最適化された ACL は、元の ACL と論理的に同等です。

ACL の最適化では、冗長 ACE の削除、ACE のマージ、および ACE の並べ替えが行われます。冗長 ACE を削除して、ACE をマージすると、TCAM エントリ数が削減されます。ACE を並べ替えると、TCAM エントリ数および TCAM マスク数が削減されます。

ACL 統計情報は、最適化された ACL を構成する ACE のカウンタから取得されます。これらの ACE は、マッピング機能によって、元のユーザ定義 ACL に対応する ACE にマッピングされます。

（注）PFC2 および PFC3A では、カウンタはソフトウェア サンプリングに基づいて行われるため、不正確です。PFC3B/PFC3BXL では、ハードウェア カウンタを使用して、正確な統計情報を提供します。PFC2/PFC3A では、カウンタは 300 ms のウィンドウ中に特定の ACE と一致したかどうかを報告しますが、エントリに一致したトラフィック数は示しません。たとえば、1000 パケット / 秒と 10 パケット / 秒の 2 つのフローがある場合、PFC2/PFC3A では両方のフローが同じ結果を戻します。PFC3B/PFC3BXL 以降の PFC には、このような制限がありません。

（注）ACL をアクティブ / スタンバイ TCAM に同時にプログラミングすることはできないため、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジン間で ACL 統計情報が異なることがあります。ただし、TCAM のプログラミング後に、トラフィックと TCAM との一致が開始すると、ACL 統計情報が同じになります。

CLI からの ACL 統計情報の設定

ここでは、次の手順について説明します。

- ACL 単位の ACL 統計情報のイネーブル化（p.15-85）
- VLAN 単位の ACL 統計情報のイネーブル化（p.15-86）
- ACE 単位の ACL 統計情報のイネーブル化（p.15-87）
- ACL 統計情報の消去（p.15-87）
- ACL 統計情報の表示（p.15-88）

ACL 単位の ACL 統計情報のイネーブル化

（注）　ARP ACE エントリは ACL マージ後に追加され、常に TCAM リスト内の最初の ACE になるため、ARP エントリ統計情報収集は常にイネーブルです。

ACL 単位でまたはすべての ACL に対して集約 ACL 統計情報をイネーブルにするには、**set security acl statistics** {*acl_name* | **all**} コマンドを入力します。集約統計情報モードでは、指定された ACL 内のすべての ACE に対して統計情報がイネーブルです。このコマンドが有効になるのは、**commit** コマンドを入力して、すべての ACE を NVRAM にコミットした場合のみです。

（注）　**set security acl statistics** {*acl_name* | **all**} コマンドは、ACE 単位コマンドの **set security acl ip/mac** *acl_name* … [**statistics**] を上書きします。

（注）　集約統計情報モードではマージ最適化がディセーブルになり、多数の ACE が使用されることがあります。場合によっては、集約統計情報モードをイネーブルにしたあとで、TCAM に導入済みの ACL が TCAM に収まらなくなることがあります。

集約 ACL 統計情報を ACL 単位でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
集約 ACL 統計情報を ACL 単位でイネーブルにします。	**set security acl statistics** {*acl_name* | **all**}

次に、集約 ACL 統計情報を ACL 単位でイネーブルにする例を示します。

```
Console> (enable) set security acl statistics ACL1
ACL1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) commit security acl ACL1
ACL commit in progress.

ACL 'ACL1' successfully committed.
Console> (enable)

Console> (enable) show security acl info ACL1
set security acl ip ACL1 statistics
--------------------------------------------------
arp permit
1. permit ip any any
Console> (enable)
```

VLAN 単位の ACL 統計情報のイネーブル化

ACL 統計情報を VLAN 単位でイネーブルにするには、**set security acl map** *acl-name* {*vlan*/*mod_port*} [**statistics enable | disable**] コマンドを入力します。

（注）VLAN モードでは、ラベル共有がディセーブルです。たとえば、特定の ACL が 10 個の VLAN にマッピングされている場合に、そのうちの 1 つの VLAN で VLAN 単位の統計情報をイネーブルにすると、9 つの VLAN でラベルが共有されます。VLAN 統計情報をイネーブルにした VLAN では別のラベルが使用されますが、これは統計情報がイネーブルであることを意味しません。マッピングした ACL に関して統計情報がイネーブルでない場合（ACE 単位または ACL 単位）、ARP パケットを除いて、統計情報は表示されません。

VLAN 上で VLAN 単位統計情報がイネーブルの場合は、同じ VLAN に設定されたこれ以降のマップでも、VLAN 単位統計情報がイネーブルになります。VLAN 上で VLAN 単位統計情報がディセーブルの場合は、同じ VLAN に設定された以前のマップでも VLAN 単位統計情報がディセーブルになります。

たとえば、**set security acl map ip1 1 statistics enable** コマンドを入力して、そのあとに **set security acl map mac1 1** コマンドを入力した場合、mac1 ACL でも VLAN 単位の統計情報はイネーブルになります。

set security acl map ip1 1 statistics enable コマンドを入力して、そのあとに **set security acl map mac1 1 statistics disable** コマンドを入力した場合は、ip1 ACL でも VLAN 単位統計情報がディセーブルになります。

ACL 統計情報を VLAN 単位でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 統計情報を VLAN 単位でイネーブルにします。	**set security acl map** *acl-name* {*vlan*/*mod_port*} [**statistics enable	disable**]
設定を表示します。	**show security acl**

次に、ACL 統計情報を VLAN 単位でイネーブルにする例を示します。

```
Console> (enable) set security acl map ACL1 1 statistics enable
Mapping in progress.

ACL ACL1 successfully mapped to VLAN 1.
Console> (enable)

Console> (enable) show security acl info ACL1
set security acl ip ACL1 statistics
---------------------------------------------------
arp permit
1. permit ip any any
Console> (enable)
```

ACE 単位の ACL 統計情報のイネーブル化

ACL 統計情報を ACE 単位でイネーブルにするには、**set security acl ip/mac** *acl_name* … [**statistics**] コマンドを入力します。このオプションを使用すると、ACL 統計情報がイネーブルでない場合にも、設定された ACE に関する統計情報を収集できます。このコマンドが有効になるのは、**commit** コマンドを入力して、すべての ACE を NVRAM にコミットした場合のみです。

ACL 統計情報を ACE 単位でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ACL 統計情報を ACE 単位でイネーブルにします。	**set security acl ip/mac** *acl_name* … [**statistics**]

次に、ACL 統計情報を ACE 単位でイネーブルにする例を示します。

```
Console> (enable) set security acl ip ACL1 permit ip any any statistics
ACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl ACL1
ACL commit in progress.

ACL 'ACL1' successfully committed.
Console> (enable)

Console> (enable) show security acl info ACL1
set security acl ip ACL1 statistics
--------------------------------------------------
arp permit
1. permit ip any any
2. permit ip any any statistics
Console> (enable)
```

ACL 統計情報の消去

ACL 統計情報を消去するには、ここに記載されたコマンドを使用します。

- **clear security acl statistics** *acl_name*

  指定された ACL のすべての ACE に対して、統計情報収集をディセーブルにします。このコマンドが有効なのは、ACL 単位で設定された ACL 統計情報のみです。VLAN 単位または ACE 単位で設定された ACL 統計情報には、このコマンドは無効です。このコマンドが有効になるのは、**commit** コマンドを入力して、すべての ACE を NVRAM にコミットした場合のみです。

  次に例を示します。

  ```
  Console> (enable) clear security acl statistics ACL1
  ACL1 editbuffer modified. Use 'commit' command to save changes.
  Console> (enable) commit security acl ACL1
  ACL commit in progress.

  ACL 'ACL1' successfully committed.
  Console> (enable)
  ```

- **clear security acl counters**

  すべての統計情報カウンタを消去します。

  次に例を示します。

  ```
  Console> (enable) clear security acl counters
  Operation Successful.
  Console> (enable)
  ```

ACL 統計情報の表示

ACL 統計情報を表示するには、ここに記載されたコマンドを使用します。

- **show security acl info** *acl_name* [**statistics** [*ace_index*]]

  指定された ACL の統計情報を表示します。*ace_index* は ACL リスト（コミットされた ACL）のインデックスです。

  次に例を示します。

```
Console> (enable) show security acl info ACL1 statistics
Vlan: 1
set security acl ip ACL1 statistics
--------------------------------------------------
arp permit in: 132 out: 132
1. permit ip any any
2. permit ip any any statistics  in: 0 out: 0

Console> (enable)
```

- **show security acl tcam interface** *vlan*

  指定された VLAN に関する TCAM の詳細を表示します。

  次に例を示します。

```
Console> (enable) show security acl tcam interface 1
Input
0. permit arp (matches 45745)
1. deny (l3) tcp any any fragment (matches 0)
2. deny (l3) ip host 21.0.0.130 any (matches 0)
3. deny (l3) udp 1.2.2.0 0.0.0.255 any (matches 0)
4. deny (l3) tcp any any 2001 (matches 0)
5. deny (l3) ip host 21.0.0.128 any (matches 0)
6. deny ip any any (matches 3)


Output
0. permit arp (matches 0)
1. deny (l3) tcp any any fragment (matches 0)
2. deny (l3) ip host 21.0.0.130 any (matches 0)
3. deny (l3) udp 1.2.2.0 0.0.0.255 any (matches 0)
4. deny (l3) tcp any any 2001 (matches 0)
5. deny (l3) ip host 21.0.0.128 any (matches 0)
6. deny (l3) ip any any (matches 0)
Console> (enable)
```

  フィールドの説明は次のとおりです。

  - deny (l3)：レイヤ 3 トラフィックが拒否され、レイヤ 2 トラフィックは許可されます。
  - redirect (l3)：レイヤ 3 トラフィックだけがリダイレクトされます。
  - bridge：このエントリに一致したトラフィックがブリッジされます。
  - Redirect (adj)：隣接情報によってトラフィックが書き替えられます。

- **show security acl** および **show security acl map** *acl_name*

  これらのコマンドに、特定の ACL または VLAN に対してイネーブルにされた統計情報のタイプを表示する新しいフィールドが追加されています。

次に例を示します。

```
Console> (enable) show security acl
Information in the bracket.
   Disable - statistics are not enabled per ACL
   Enable - stats are enabled per ACL
   The number shows the VLANs where per-vlan stattistics are enabled
ACL                                Type VLANS (Statistics)
--------------------------------   ---- ----------------
ip1                                IP   2-9    (2-3 Enable)
ip2                                IP   10     (Disable)
ip3                                IP   11     (Disable)
Console> (enable)
```

フィールドの説明は次のとおりです。

- Disable：ACL で統計情報がディセーブルです。
- Enable：ACL で統計情報がイネーブルです。
- 番号は VLAN 単位の統計情報がイネーブルになっている VLAN を示します（例の [2-3] など）。

CRAM の設定

Compression and Reordering of the ACL Mask（CRAM）機能は、複数の ACL にわたってマスク使用率を最適化します。この最適化によりマスク共有が促進され、TCAM の使用効率が高まり、TCAM 内にさらに多くの ACL をプログラミングできます。

TCAM はハードウェアに ACL を実装する場合に使用されます。8 つの値エントリで 1 つのマスクエントリが共有されます。ACL をプログラミングする場合に、TCAM が一杯であると、エラーが表示され、TCAM ハードウェアに新規 ACL をプログラミングできなくなります。この問題は通常、TCAM マスクの不足が原因で発生します。

CRAM は 2 つのモードで実行できます。手動モードでは、この機能を必要に応じて実行します。自動モードでは、TCAM が一杯となる例外状況が発生した場合に、この機能が実行されます。この機能が実行されると、新規のマスク順序が計算され、ACL ハードウェアがそれに応じてプログラミングされます。

（注）　Release 8.4(1) では、CRAM はセキュリティ ACL でのみサポートされています。この機能は QoS ACL で有効ですが、QoS ACL 専用に実行することはできません。

CLI からの CRAM 機能の設定

（注）　CRAM 機能を実行すると、ハードウェア プログラミング中に 0.5 秒未満の間、トラフィックが中断（拒否）されます。

ここでは、次の手順について説明します。

- CRAM 機能のテスト実行のイネーブル化（p.15-90）
- CRAM 機能の手動によるイネーブル化（p.15-91）
- CRAM 機能の自動実行のイネーブル化（p.15-91）
- CRAM 機能のステータス情報の表示（p.15-92）
- CRAM 機能の自動モードのディセーブル化（p.15-92）

CRAM 機能のテスト実行のイネーブル化

ACL マスクの使用の有無を判別するには、**set security acl cram testrun** コマンドを入力します。このコマンドは単なる情報用です。ソフトウェア構造やハードウェア構造は変更されず、トラフィックは中断されません。

CRAM 機能のテスト実行をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM 機能のテスト実行をイネーブルにします。	**set security acl cram testrun**

次に、CRAM 機能のテスト実行をイネーブルにする例を示します。

```
Console> (enable) set security acl cram testrun
CRAM execution in progress.

CRAM execution complete.
Current ACL storage mask usage 60.0%
ACL storage mask usage if CRAM is run is 41.0%
Console> (enable)
```

CRAM 機能の手動によるイネーブル化

CRAM 機能を手動でイネーブルにするには、**set security acl cram run** コマンドを入力します。

CRAM 機能を手動でイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM 機能を手動でイネーブルにします。	**set security acl cram run**

次に、手動で CRAM 機能をイネーブルにする例を示します。

```
Console> (enable) set security acl cram run
Traffic may be disrupted for some time while programming hardware. Agree (y/n)[n] ? y
CRAM execution in progress.

CRAM execution complete.
Previous ACL storage mask usage 60.0%
Current ACL storage mask usage 41.0%
Console> (enable)
```

CRAM 機能の自動実行のイネーブル化

CRAM 機能の自動実行をイネーブルにするには、**set security acl cram auto** [*nsec*] コマンドを入力します。自動実行がイネーブルの場合、この機能は TCAM が一杯になると自動的に実行されます。デフォルトのタイマー設定は 300 秒です。*nsec* は 60 ～ 3600 秒に指定できます。前回この機能を実行してから TCAM が変更されていない場合は、この機能が自動実行されません。

CRAM 機能の自動実行をイネーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM 機能の自動実行をイネーブルにします。	**set security acl cram auto** [*nsec*]

次に、CRAM 機能の自動実行をイネーブルにする例を示します。

```
Console> (enable) set security acl cram auto
Cram auto mode enabled. Timer is default =  300 seconds
Console> (enable)

Console> (enable) set security acl cram auto 1000
Cram auto mode enabled. Timer is 1000 seconds
Console> (enable)
```

CRAM 機能のステータス情報の表示

CRAM 機能のステータス情報を表示するには、**show security acl cram** コマンドを入力します。

CRAM 機能のステータス情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
CRAM 機能のステータス情報を表示します。	**show security acl cram**

次に、CRAM 機能のステータス情報を表示する例を示します。

```
Console> (enable) show security acl cram
Cram auto mode is enabled. Timer is 300.
Cram last run on Fri Jun 18 2004, 10:06:29
Security ACL mask usage before: 0.17%
Security ACL mask usage after: 0.12%
Total number of cram executions = 2
Console> (enable)
```

CRAM 機能の自動モードのディセーブル化

CRAM の自動モードをディセーブルにするには、**clear security acl cram auto** コマンドを入力します。

CRAM の自動モードをディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
CRAM の自動モードをディセーブルにします。	**clear security acl cram auto**

次に、CRAM の自動モードをディセーブルにする例を示します。

```
Console> (enable) clear security acl cram auto
Cram auto mode disabled.
Console> (enable)
```

PBF の設定

Policy-Based Forwarding（PBF）機能は、PFC2 および PFC3A/PFC3B/PFC3BXL によってサポートされる VACL リダイレクションの拡張機能です。PBF が特に有効なのは、トランスペアレント ブリッジングに使用され、必要な VLAN 間通信の量が限られているフラットなレイヤ 2 ネットワークや、ブリッジング装置（サーバのロードバランシング装置など）が含まれていたり、ファイアウォールのロードバランシングが実行されていたりするサーバ ファームまたは Demilitarized Zone（DMZ; 非武装地帯）です。

（注）Release 7.5(1) 以降のソフトウェア リリースでは PBF 機能が拡張され、セキュリティ ACL と隣接情報の設定およびコミットのプロセスが簡略化されています。詳細は、「PBF 設定の拡張機能（Releases 7.5(1) 以降のソフトウェア リリース）」（p.15-105）を参照してください。

（注）Release 8.3(1) 以降のソフトウェア リリースではさらに PBF 機能が拡張され、セキュリティ ACL と隣接情報の設定およびコミットのプロセスが簡略化されています。詳細は、「PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）」（p.15-108）を参照してください。

（注）PBF は、IPX およびマルチキャスト トラフィックをサポートしていません。

（注）PBF は、802.1Q トンネル トラフィックでは機能しません。PBF はレイヤ 3 IP ユニキャスト トラフィックではサポートされていますが、レイヤ 2 トラフィックには適用されません。中間（PBF）スイッチでは、802.1Q トンネル トラフィックはすべてレイヤ 2 トラフィックとみなします。

（注）PBF は、接続したホスト上で設定が必要になる場合があります。ネットワークにルータが存在しない場合は、PBF に参加する各ホストに対して ARP テーブル エントリを静的に追加する必要があります。

ここでは、PBF について説明します。

PBF の機能概要

PBF の設定には、次の作業が必要です。

- PBF のイネーブル化と PFC2 または PFC3A/PFC3B/PFC3BXL 用 MAC アドレスの指定
- PBF のための VACL の設定
- PBF のための接続ホストの設定

PFC2 または PFC3A/PFC3B/PFC3BXL 用 MAC アドレスを指定することで PBF をイネーブルにできます。MAC アドレスは、デフォルト設定のものでもユーザ側で指定する MAC アドレスでもかまいません。パケットを送信する場合は、宛先 MAC アドレスは PFC2 または PFC3A/PFC3B/PFC3BXL MAC アドレスと同じでなければなりません。PFC2 または PFC3A/PFC3B/PFC3BXL は、パケットがレイヤ 3 のパケットであると認識する必要があります。認識しない場合は書き換え処理が行われません。パケットに PFC2 または PFC3A/PFC3B/PFC3BXL MAC アドレスが設定されないで送信された場合、PFC2 または PFC3A/PFC3B/PFC3BXL はこれらのパケットをレイヤ 2 パケットとして処理します。

PBF VACL は **set security acl** コマンドを使用して作成されます。PBF VACL は、PFC2 または PFC3A/PFC3B/PFC3BXL の隣接テーブル エントリとリダイレクト ACE を含みます。PBF に参加している両方の VLAN に対して VACL を設定する必要があります。送信元 VLAN からのパケットが PFC2 または PFC3A/PFC3B/PFC3BXL に着信し、PBF VACL に一致します。隣接テーブルに記入されている情報に基づいてパケット ヘッダーが書き換えられ（宛先 VLAN および送信元と宛先の MAC アドレス）、パケットは宛先 VLAN に転送されます。パケットは、隣接情報に対応付けられた VACL エントリに一致した場合にだけ、VLAN 間で転送されます。

（注）　VACL は着信および発信トラフィックに適用されるので、PBF を使用する場合はすべての VACL を慎重に設定する必要があります。VACL が特定されていない場合は、書き換えられたパケットが発信 VACL の deny（拒否）ステートメントと一致し、廃棄される可能性があります。

ネットワークにルータが存在しない場合は、参加しているホスト上でスタティック ARP エントリを指定する必要があります。

PBF のハードウェアおよびソフトウェア要件

PBF のハードウェアおよびソフトウェアの要件は、次のとおりです。

- PBF には、PFC2 搭載の Supervisor Engine 2、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720、または PFC3B/PFC3BXL 搭載の Supervisor Engine 32 が必要です。
- PBF は、PBF 用に使用されている Catalyst 6500 シリーズ スイッチで動作する（起動済み）MSFC2、MSFC2A、または MSFC3 ではサポート*されていません。*

  MSFC2、MSFC2A、または MSFC3 が存在して起動した状態で PBF を設定しようとすると、システムはその機能が MSFC2、MSFC2A、または MSFC3 でサポートされていないことを示すメッセージを返します。

  MSFC2、MSFC2A、または MSFC3 が存在していても起動していない場合は、PBF を設定できます。
- Supervisor Engine 2 の場合、PBF にはスーパバイザ エンジン Release 6.3(1) 以降のソフトウェア リリースが必要です。
- Supervisor Engine 720 の場合、PBF にはスーパバイザ エンジン Release 8.1(1) 以降のソフトウェア リリースが必要です。
- Supervisor Engine 32 の場合、PBF にはスーパバイザ エンジン Release 8.4(1) 以降のソフトウェア リリースが必要です。

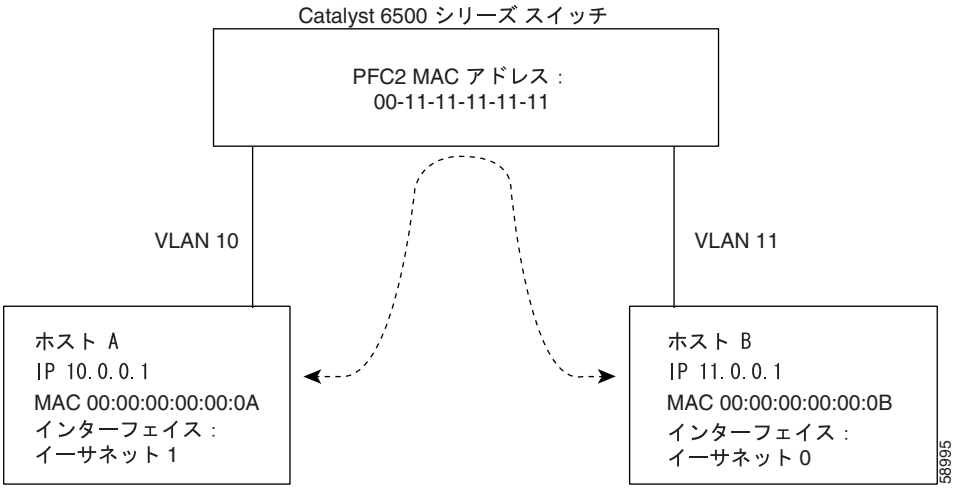
CLI からの PBF の設定

（注）　ここでの注意事項および構成例の詳細については、「PBF 設定の拡張機能（Releases 7.5(1) 以降のソフトウェア リリース）」（p.15-105）および「PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）」（p.15-108）を参照してください。

ここでは、PBF 設定時の注意事項と設定例について説明します。設定例は、図 15-10 の例を参照してください。Catalyst 6500 シリーズ スイッチは、VLAN 10 のホスト A からのトラフィックをすべて VLAN 11 のホスト B にリダイレクトし、ホスト B からのトラフィックをホスト A にリダイレクトします。ここでは PBF の設定手順について説明します。

- PBF のイネーブル化と PFC2 または PFC3A/PFC3B/PFC3BXL 用 MAC アドレスの指定（p.15-95）
- VLAN における PBF MAC アドレスの指定（p.15-97）
- PBF のための VACL の設定（p.15-98）
- PBF 情報の表示（p.15-100）
- PBF VACL のエントリの削除（p.15-100）
- 編集バッファ内の隣接テーブル エントリのロール バック（p.15-101）
- PBF のためのホストの設定（p.15-101）

図 15-10　PBF



PBF のイネーブル化と PFC2 または PFC3A/PFC3B/PFC3BXL 用 MAC アドレスの指定

（注）　MAC アドレスは、デフォルト設定のものでもユーザ側で指定する MAC アドレスでもかまいません。デフォルトの MAC アドレスは、Catalyst 6500 シリーズ スイッチ シャーシの MAC アドレス PROM から取得します。**set pbf mac** コマンドで MAC アドレスを指定する場合は、必ず MAC アドレスは一意のもので、どのインターフェイス上でも未使用であることを確認してください。

MAC アドレス PROM から取得するデフォルトの MAC アドレスを使用することを推奨します。**set pbf mac** コマンドで独自の MAC アドレスを指定する場合、その MAC アドレスが使用中のものと重複すると、パケットが廃棄されることがあります。

PBF のステータスと MAC アドレスを表示するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF のステータスと MAC アドレスを表示します。	**show pbf**

PBF をイネーブルにするには、イネーブル モードで次のいずれかの作業を行います。

作業	コマンド
デフォルトの MAC アドレスで PBF をイネーブルにします。	**set pbf**
特定の MAC アドレスで PBF をイネーブルにします。	**set pbf** [**mac** *mac_address*]

次に、PBF のステータスと MAC アドレスをチェックし、デフォルトの MAC アドレスで PBF をイネーブルにし、設定を確認する例を示します。

```
Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
not set       00-00-00-00-00-00
Console> (enable)
Console> (enable) set pbf
PBF committed successfully.
Operation successful.
Console> (enable)
Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-01-64-61-39-c2
Console> (enable)
```

次に、特定の MAC アドレスで PBF をイネーブルにする例を示します。

```
Console> (enable) set pbf mac 00-11-11-11-11-11
PBF committed successfully.
Operation successful.
Console> (enable)

Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-11-11-11-11-11
Console> (enable)
```

PBF をディセーブルにして PBF MAC アドレスを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF をディセーブルにして PBF MAC アドレスを消去します。	**clear pbf**

次に、PBF MAC アドレスを削除する例を示します。

```
Console> (enable) clear pbf
PBF cleared.
Console> (enable)

Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
not set       00-00-00-00-00-00
Console> (enable)
```

VLAN における PBF MAC アドレスの指定

（注）　この PBF 設定手順は、PFC3A/PFC3B/PFC3BXL 搭載の Supervisor Engine 720 上でのみ必要です。

set pbf vlan *vlan* コマンドを実行すると、指定した VLAN 上の PBF レイヤ 2 CAM（連想メモリ）エントリが作成されます。これらのエントリに一致するパケットは、レイヤ 3 パケットとして分類されます。レイヤ 2 エントリが作成されるのは、**set pbf vlan** コマンドを使用する前に **set pbf mac** コマンドを使用して PBF MAC アドレスを設定する場合だけです。

VLAN 上の PBF MAC アドレスを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
VLAN 上の PBF MAC アドレスを指定します。	**set pbf vlan** *vlan*

次に、VLAN 上の PBF MAC アドレスを指定する例を示します。

```
Console> (enable) set pbf vlan 11-12
Console> (enable) PBF enabled on vlan(s) 11-12.
Operation successful.
Console> (enable) show pbf
Pbf status    Mac address            Vlans
-----------   ------------------     ---------
ok            00-01-64-f8-39-18      11-12
Console> (enable)
```

メッセージ [Operation successful] は、PBF MAC アドレスが NVRAM に保存されたことを示します。

clear pbf コマンドを入力しても、PBF がイネーブルにされた VLAN は消去されません。**clear pbf** コマンドを実行すると、その VLAN に対応付けられたレイヤ 2 テーブル エントリは（MAC アドレスが有効でなくなるため）消去されます。NVRAM から PBF 対応 VLAN を削除するには、**clear pbf vlan** *vlan_list* コマンドを入力して、目的の VLAN を明示的に消去する必要があります。

PBF のための VACL の設定

（注）　**set security acl adjacency** コマンドを使用して隣接テーブルの書き換え情報を指定します。この情報により、パケット ヘッダーが書き換えられ（宛先 VLAN および送信元と宛先の MAC アドレス）、宛先 VLAN に転送されます。

送信元 MAC アドレスの指定は任意です。送信元 MAC アドレスを指定しなかった場合は、システムによりデフォルトで PBF MAC アドレスに設定されます。

（注）　VLAN には最大 256 の隣接テーブル エントリを設定できます。隣接テーブル エントリの最大数は 1023 です。

（注）　PBF を使用してジャンボ フレーム転送をイネーブルにするには、**set security acl adjacency** コマンドで **mtu** キーワードを使用します。

PBF VACL でのエントリの順序は重要です。隣接テーブル エントリは、リダイレクト ACE によりトラフィックのリダイレクトに使用されるので、リダイレクト ACE より先に定義する必要があります。PBF VACL のエントリは、次の順序で作成してください。

1. 隣接テーブル エントリを指定します。
2. 隣接テーブル エントリを使用する PBF VACL のリダイレクト ACE を指定します。
3. 隣接テーブル エントリをコミットします。
4. PBF VACL をコミットします。
5. PBF VACL を 1 つまたは複数の VLAN にマッピングします。

ヒント　**commit security acl all** コマンドを使用すると、ステップ 3 およびステップ 4 をまとめることができます。

（注）　複数のリダイレクト ACE で同じ隣接テーブル エントリを使用できます。

PFC2 または PFC3A/PFC3B/PFC3BXL 用の隣接テーブル エントリを指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
PFC2 または PFC3A/PFC3B/PFC3BXL 用の隣接テーブル エントリを指定します。	**set security acl adjacency** *adjacency_name dest_vlan dest_mac* [[*source_mac*] | [*source_mac* **mtu** *mtu_size*] | [**mtu** *mtu_size*]]

次に、隣接テーブル エントリを指定する例を示します。

```
Console> (enable) set security acl adjacency ADJ1 11 00-00-00-00-00-0B
ADJ1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

次に、VLAN 10 の PBF VACL を作成する例を示します（図 15-10 を参照）。

```
Console> (enable) set security acl adjacency ADJ1 11 00-00-00-00-00-0B
ADJ1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL1 redirect ADJ1 ip host 10.0.0.1 host
11.0.0.1
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL1 permit any
IPACL1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl adjacency
Commit operation in progress.

Adjacency successfully committed.
Console> (enable) commit security acl IPACL1
ACL commit in progress.

ACL 'IPACL1' successfully committed.
Console> (enable) set security acl map IPACL1 10
Mapping in progress.

ACL IPACL1 successfully mapped to VLAN 10.
Console> (enable)
```

次に、VLAN 11 の PBF VACL を作成する例を示します（図 15-10 を参照）。

```
Console> (enable) set security acl adjacency ADJ2 10 00-00-00-00-00-0A
ADJ2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL2 redirect ADJ2 ip host 11.0.0.1 host
10.0.0.1
IPACL2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) set security acl ip IPACL2 permit any
IPACL2 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl adjacency
Commit operation in progress.

Adjacency successfully committed.
Console> (enable) commit security acl IPACL2
ACL commit in progress.

ACL 'IPACL2' successfully committed.
Console> (enable) set security acl map IPACL2 11
Mapping in progress.

ACL IPACL2 successfully mapped to VLAN 11.
Console> (enable)
```

PBF 情報の表示

ここでは、PBF 関連情報の表示方法について説明します。

隣接テーブル エントリを表示するには、ユーザ モードで次のいずれかの作業を行います。

作業	コマンド
隣接テーブル エントリを表示します。	**show security acl info** [*acl_name* | **adjacency** | **all**] [**editbuffer** [*editbuffer_index*]]
すべての隣接テーブル エントリまたは特定の隣接テーブル エントリに対する PBF 隣接情報を表示します。	**show pbf adjacency** [*adj_name*]
すべての隣接テーブル エントリまたは特定の隣接テーブル エントリに対する PBF 統計情報を表示します。	**show pbf statistics** [*adj_name*]
すべての隣接テーブル エントリまたは特定の隣接テーブル エントリに対する隣接 /VACL マッピングを表示します。	**show pbf map** [*adj_name*]

次に、隣接テーブル エントリを表示する例を示します。

```
Console> show security acl info adjacency
set security acl adjacency ADJ1
---------------------------------------------------
1. 11 00-00-00-00-00-0b

set security acl adjacency ADJ2
---------------------------------------------------

1. 10 00-00-00-00-00-0a
Console> show pbf adjacency
Index    DstVlan   DstMac             SrcMac             Name
-----------------------------------------------------------------
1        11      00-00-00-00-00-0a  00-00-00-00-00-0b     ADJ1
2        10      00-00-00-00-00-0a  00-00-00-00-00-0b     ADJ2
Console> show pbf statistics
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-------------------------------------------------------------------------
1        11      00-00-00-00-00-0a  00-00-00-00-00-0b  0x00000000    ADJ1
2        10      00-00-00-00-00-0a  00-00-00-00-00-0b  0x00000000    ADJ2
Console> show pbf map
Adjacency            ACL
------------------  --------------------
ADJ1                IPACL1

ADJ2                IPACL2
Console> (enable)
```

PBF VACL のエントリの削除

リダイレクト ACE より先に隣接テーブルを消去することはできません。PBF VACL のリダイレクト ACE および隣接テーブル エントリを消去する場合は、次の順序で行ってください。

1. リダイレクト ACE を消去します。
2. PBF VACL をコミットします。
3. 隣接テーブル エントリを消去します。
4. 隣接テーブル エントリをコミットします。

PBF 隣接テーブル エントリを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF 隣接テーブル エントリを消去します。	**clear security acl adjacency** *adj name*

次に、PBF 隣接テーブル エントリを削除する例を示します。

```
Console> (enable) clear security acl adjacency ADJ1
Adj is in use by a VACL, clear the VACL first then clear adj.
Console> (enable) clear security acl IPACL1
IPACL1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) commit security acl IPACL1
ACL commit in progress.

ACL 'IPACL1' successfully deleted.
Console> (enable) clear security acl adjacency ADJ1
ADJ1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl adjacency
Console> (enable) Adjacency committed successfully
Commit operation in progress.

Console> (enable)
```

編集バッファ内の隣接テーブル エントリのロール バック

rollback コマンドを使用して、最後のコミット以前に編集バッファ内に作成された隣接テーブル エントリを削除できます。隣接テーブル エントリは、最後のコミットでのステートにロール バックされます。

編集バッファ内の隣接テーブル エントリをロール バックするには、イネーブル モードで次の作業を行います。

作業	コマンド
編集バッファ内の隣接テーブル エントリをロール バックします。	**rollback security acl** {*acl_name* | **all** | **adjacency**}

次に、編集バッファ内の隣接テーブル エントリをロール バックする例を示します。

```
Console> (enable) rollback security acl adjacency
Editbuffer for adjacency info rolled back to last commit state.
Console> (enable)
```

PBF のためのホストの設定

ここでは、次のプラットフォームおよび OS（オペレーティング システム）のホスト設定手順について説明します。

- Linux（p.15-102）
- Sun ワークステーション（p.15-102）
- MS-Windows/NT/2000 ホスト（p.15-103）

（注）ネットワークにルータが存在しない場合は、参加しているホスト上でスタティック ARP エントリを指定する必要があります。ホストの ARP テーブルは、ホスト装置の IP アドレスを PFC2 または PFC3A/PFC3B/PFC3BXL の MAC アドレスにマッピングします。

（注）　次の例の IP アドレスは、図 15-10 で使用される IP アドレスです。これらのアドレスは任意に選択されたものです。ネットワーク構成で使用する IP アドレスが一意のものであることを確認してください。

Linux

次に、Linux OS（オペレーティング システム）が稼働するホストに ARP テーブルを設定する例を示します。

ホスト A を設定する例を示します。

```
arp -s 11.0.0.1 00:11:11:11:11:11 -i eth0
route add 11.0.0.1 eth0
```

ホスト B を設定する例を示します。

```
arp -s 10.0.0.1 00:11:11:11:11:11 -i eth1
route add 10.0.0.1 eth1
```

Sun ワークステーション

PBF を使用して Sun ワークステーションのエンド ホストで 2 つの VLAN 間における転送をイネーブルにする場合は、ホスト設定時に考慮すべき制限事項があるので注意してください。

- PBF の制限事項

  PBF は ARP をサポートしていません。PBF に参加する Sun ワークステーションごとにスタティック ARP エントリを設定する必要があります。各スタティック ARP エントリは、宛先ホストにマッピングされた PBF MAC アドレスを示す必要があります。

  また、Sun ワークステーションにゲートウェイを設定することも必要です。Sun ワークステーションが異なるネットワークと通信する必要がある場合は、PBF を通過するすべてのネットワークに対するホスト ルートを定義する必要があります。また、必要に応じてデフォルトのゲートウェイを定義する必要があります。

  たとえば、VLAN 40 のホスト 10.0.0.1 が VLAN 50 のホスト 11.0.0.1 と通信する必要があり、PBF MAC アドレスが 00-11-11-11-11-11 である場合、スタティック ARP エントリは次のようになります。

  ```
  arp -s 11.0.0.1 00:11:11:11:11:11
  ```

  この場合、00-11-11-11-11-11 は PBF MAC アドレスであり、11.0.0.1 は宛先ホストの IP アドレスです。

- Sun ワークステーションの制限事項

  Sun ワークステーションでは、宛先が別のネットワークの一部である場合（上記の例では 11.x.x.x）、スタティック ARP エントリを設定できません。これはすべての Sun ワークステーションでの ARP の制限事項です。この問題を解決するには、ホスト ルートであるダミー ゲートウェイを定義し、宛先ホストにマッピングされた PBF MAC アドレスを示すスタティック ARP エントリを設定する必要があります。

  上の例を使用して、最初にゲートウェイに対するダミー スタティック ARP エントリを定義する必要があります。ゲートウェイの IP アドレスは、そのネットワーク内のホスト アドレスのいずれかです。

  ```
  (A)Kubera# arp -s 10.0.0.2  00:11:11:11:11:11
  (B)Kubera# route add host  11.0.0.1 10.0.0.2
  ```

  PBF 関連トラフィックのダミー ARP エントリを 1 つと、各宛先ホストのホスト ルートを設定するだけです。

ホスト数が増えた場合は、各宛先ホストについてホスト ルート エントリを設定する必要があります。各宛先ホストのホスト ルート エントリがある /etc/rc2.d に、スタートアップ ファイルを設定できます。このファイルを設定すると、Sun ワークステーションをリセットまたは再起動したあと、すべてのホスト ルートを入力する必要がなくなります。

ファイルのエントリは次の形式を使用します。

```
Route add host <destination Host IP Address> <dummy gateway IP Address>
```

スタートアップ スクリプトの 1 つとしてホスト ルート エントリが記述されているファイルを使用する必要があります。ルート / スーパユーザのフルアクセス権を持つディレクトリにファイルを作成したり、/etc/rc2.d 内のそのファイルを示すソフト リンクを設定したり、あるいは /etc/rc2.d ディレクトリ自体にファイルを作成することもできます。

MS-Windows/NT/2000 ホスト

Windows ベースの PC 上にスタティック ARP エントリを設定する必要があります。Windows ベースの PC では、PBF を使用する VLAN 間のスイッチングのためのダミー ゲートウェイを設定する必要はありません。

次に、Windows ベースのプラットフォームにスタティック ARP エントリを設定する例を示します。

```
C:\> arp -s 11.0.0.1 00-11-11-11-11-11
```

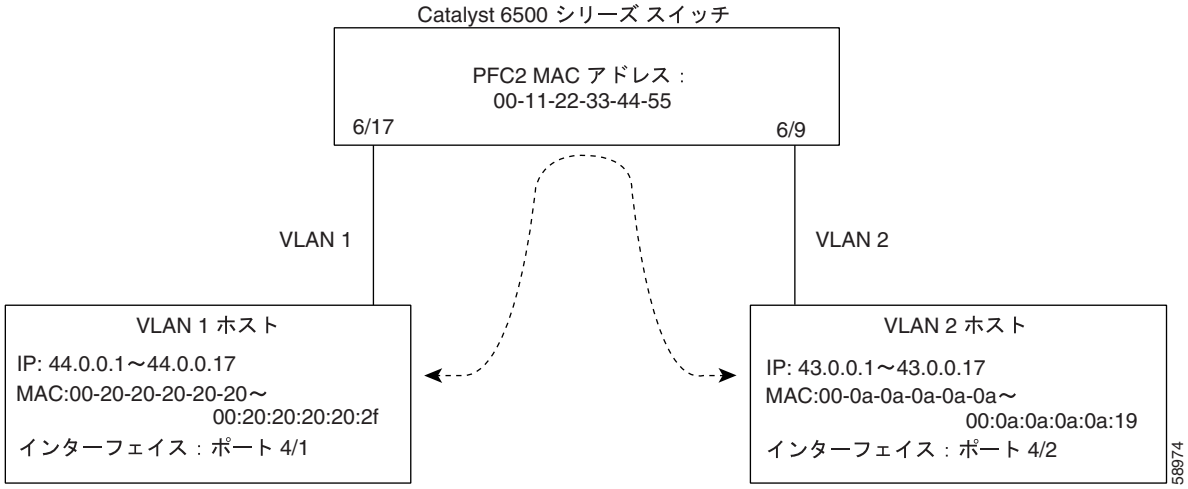
この例では、00-11-11-11-11-11 は PBF MAC アドレスであり、11.0.0.1 は宛先ホストの IP アドレスです。

さらにホストを設定する必要がある場合は、各宛先ホストに対する ARP エントリでバッチ ファイルを作成して、Windows がこのファイルをスタートアップ時に使用するように指定できます。

PBF の設定例

ここでは、VLAN 1 のホストと VLAN 2 のホストとの間の PBF をイネーブルにする設定例を示します（図 15-11 を参照）。

図 15-11　PBF の設定例



次に、VLAN 1 上のホストと VLAN 2 上のホストとの間で PBF をイネーブルにするために作成されたスイッチ コンフィギュレーション ファイルの例を示します。この例では、各 VLAN の最初の 4 つのホストだけが表示されます（44.0.0.1 ～ 44.0.0.4 および 43.0.0.1 ～ 43.0.0.4）。

```
#security ACLs
clear security acl all
#adj set
set security acl adjacency a_1 2 00-0a-0a-0a-0a-0a
set security acl adjacency a_2 2 00-0a-0a-0a-0a-0b
set security acl adjacency a_3 2 00-0a-0a-0a-0a-0c
set security acl adjacency a_4 2 00-0a-0a-0a-0a-0d
set security acl adjacency b_1 1 00-20-20-20-20-20
set security acl adjacency b_2 1 00-20-20-20-20-21
set security acl adjacency b_3 1 00-20-20-20-20-22
set security acl adjacency b_4 1 00-20-20-20-20-23
#ip1
set security acl ip ip1 permit arp
set security acl ip ip1 redirect  a_1  ip host 44.0.0.1 host 43.0.0.1
set security acl ip ip1 redirect  a_2  ip host 44.0.0.2 host 43.0.0.2
set security acl ip ip1 redirect  a_3  ip host 44.0.0.3 host 43.0.0.3
set security acl ip ip1 redirect  a_4  ip host 44.0.0.4 host 43.0.0.4
set security acl ip ip1 permit ip any any
#ip2
set security acl ip ip2 permit arp
set security acl ip ip2 redirect  b_1  ip host 43.0.0.1 host 44.0.0.1
set security acl ip ip2 redirect  b_2  ip host 43.0.0.2 host 44.0.0.2
set security acl ip ip2 redirect  b_3  ip host 43.0.0.3 host 44.0.0.3
set security acl ip ip2 redirect  b_4  ip host 43.0.0.4 host 44.0.0.4
set security acl ip ip2 permit ip any any
#pbf set
set pbf mac 00-11-22-33-44-55
#
commit security acl all
set security acl map ip1 1
set security acl map ip2 2
```

次に、VLAN 1 上のポート 6/17 について、スイッチによって学習された MAC アドレスを表示する例を示します。

```
Console> (enable) show cam dynamic 6/17
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ---------------------------------------------
1     00-20-20-20-20-23             6/17 [ALL]
1     00-20-20-20-20-22             6/17 [ALL]
1     00-20-20-20-20-21             6/17 [ALL]
1     00-20-20-20-20-20             6/17 [ALL]
1     00-20-20-20-20-27             6/17 [ALL]
1     00-20-20-20-20-26             6/17 [ALL]
1     00-20-20-20-20-25             6/17 [ALL]
1     00-20-20-20-20-24             6/17 [ALL]
1     00-20-20-20-20-2b             6/17 [ALL]
1     00-20-20-20-20-2a             6/17 [ALL]
1     00-20-20-20-20-29             6/17 [ALL]
1     00-20-20-20-20-28             6/17 [ALL]
1     00-20-20-20-20-2f             6/17 [ALL]
1     00-20-20-20-20-2e             6/17 [ALL]
1     00-20-20-20-20-2d             6/17 [ALL]
1     00-20-20-20-20-2c             6/17 [ALL]
Total Matching CAM Entries Displayed for 6/17 = 16 for port 6/9, vlan 2
```

次に、VLAN 2 上のポート 6/9 について、スイッチによって学習された MAC アドレスを表示する例を示します。

```
Console> (enable) show cam dynamic 6/9
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ----------------------------------------
2     00-0a-0a-0a-0a-0e            6/9 [ALL]
2     00-0a-0a-0a-0a-0f            6/9 [ALL]
2     00-0a-0a-0a-0a-0c            6/9 [ALL]
2     00-0a-0a-0a-0a-0d            6/9 [ALL]
2     00-0a-0a-0a-0a-0a            6/9 [ALL]
2     00-0a-0a-0a-0a-0b            6/9 [ALL]
2     00-0a-0a-0a-0a-19            6/9 [ALL]
2     00-0a-0a-0a-0a-18            6/9 [ALL]
2     00-0a-0a-0a-0a-17            6/9 [ALL]
2     00-0a-0a-0a-0a-16            6/9 [ALL]
2     00-0a-0a-0a-0a-15            6/9 [ALL]
2     00-0a-0a-0a-0a-14            6/9 [ALL]
2     00-0a-0a-0a-0a-13            6/9 [ALL]
2     00-0a-0a-0a-0a-12            6/9 [ALL]
2     00-0a-0a-0a-0a-11            6/9 [ALL]
2     00-0a-0a-0a-0a-10            6/9 [ALL]
Total Matching CAM Entries Displayed for 6/9 = 16
```

次に、PBF ステータスと PFC2 または PFC3A/PFC3B/PFC3BXL MAC アドレスを表示する例を示します。

```
Console> (enable) show pbf
Pbf status    Mac address
-----------   ------------------
ok            00-11-22-33-44-55
```

次に、PBF 統計情報を表示する例を示します。

```
Console> (enable) show pbf statistics
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-----------------------------------------------------------------------
1         2      00-0a-0a-0a-0a-0a  00-11-22-33-44-55  0x00026d7c    a_1
2         2      00-0a-0a-0a-0a-0b  00-11-22-33-44-55  0x00026d83    a_2
3         2      00-0a-0a-0a-0a-0c  00-11-22-33-44-55  0x00026d89    a_3
4         2      00-0a-0a-0a-0a-0d  00-11-22-33-44-55  0x00026d90    a_4
5         1      00-20-20-20-20-20  00-11-22-33-44-55  0x000260e3    b_1
6         1      00-20-20-20-20-21  00-11-22-33-44-55  0x000260ea    b_2
7         1      00-20-20-20-20-22  00-11-22-33-44-55  0x000260f1    b_3
8         1      00-20-20-20-20-23  00-11-22-33-44-55  0x000260f8    b_4
```

PBF 設定の拡張機能（Releases 7.5(1) 以降のソフトウェア リリース）

ここでは、Release 7.5(1) 以降のソフトウェア リリースで利用できるコンフィギュレーション コマンドを使用して PBF を設定する手順について説明します。

ここでは、PBF 設定の拡張機能について説明します。

PBF 設定拡張機能の概要

（注）　**set pbf-map** コマンドは Release 8.3(1) で変更されました。詳細については、「PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）」（p.15-108）を参照してください。

新しい **set pbf-map** コマンドは、入力された情報に基づいてセキュリティ ACL と隣接情報を作成し、ACL を自動的にコミットします。**set pbf-map** コマンドでは、次の 2 つのステップを伴います。

ステップ 1　隣接テーブルの挿入

このステップでは、ACL に追加された各リダイレクト / 隣接 ACE について隣接テーブルにエントリを作成します。

ステップ 2　ACL の作成および変更

このステップでは、リダイレクト / 隣接エントリについて各 ACL に ACE を作成し、ACL の末尾に **permit ip any any** ACE を追加します（この ACE は、ACL にまだ **permit ip any any** ACE がない場合にだけ、追加されます）。

set pbf-map コマンドの構文は、**set pbf-map** *ip_addr_1 mac_1 vlan_1 ip_addr_2 mac_2 vlan_2* です。

簡易構文の例は、**set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 12** です。

新しい **set pbf-map** コマンドは、次の Release 7.5(1) より前のすべてのコマンドと同じです。

```
set security acl adjacency PBF_MAP_ADJ_0 11 0-0-0-0-0-1
set security acl adjacency PBF_MAP_ADJ_1 12 0-0-0-0-0-2
commit security acl adjacency
set security acl ip PBF_MAP_ACL_11 redirect PBF_MAP_ADJ_1 ip host 1.1.1.1 host 2.2.2.2
set security acl ip PBF_MAP_ACL_12 redirect PBF_MAP_ADJ_0 ip host 2.2.2.2 host 1.1.1.1
```

permit ip any any ACE がない場合は、次の 2 つの **permit ip any any** エントリが追加されます。

```
set security acl ip PBF_MAP_ACL_11 permit ip any any
set security acl ip PBF_MAP_ACL_12 permit ip any any
commit security acl ip PBF_MAP_ACL_11
commit security acl ip PBF_MAP_ACL_12
set security acl map PBF_MAP_ACL_11 11
set security acl map PBF_MAP_ACL_12 12
```

set pbf-map コマンドによって追加された ACL 内の各エントリは、デフォルトの **permit ip any any** ACE の前に挿入されます。

リダイレクト ACE 以外のエントリを隣接テーブルに追加する場合は、**set security acl ip PBF_MAP_ACL_(VLAN_ID)** コマンドを入力します。PBF_MAP_ACL_(VLAN_ID) ACL 名は、次のアルゴリズムに基づきます。つまり、対応するホストの VLAN 番号が PBF_MAP_ACL_ ストリングに追加されます。

PBF_MAP_ACL_(VLAN_ID) ACL に含まれているリダイレクト / 隣接 ACE と隣接情報を削除するには、**clear pbf-map** コマンドを入力します。PBF_MAP_ACL_(VLAN_ID) ACL の一部であるその他すべての ACE タイプを消去するには、**clear security acl** コマンドを入力します。

PBF_MAP_ACL の指定

（注）　**set pbf-map** コマンドが使用する ACL 名は、このコマンド用に予約されています。**set security acl** コマンドを入力すると、PBF_MAP_ACL で始まる名前は使用できません。隣接情報に使用される名前も、**set pbf-map** コマンド用に予約されています。**set security acl adjacency** コマンドを入力すると、PBF_MAP_ADJ で始まる名前は使用できません。

PBF_MAP_ACL を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
PBF_MAP_ACL を指定します。	**set pbf-map** *ip_addr_1 mac_1 vlan_1 ip_addr_2 mac_2 vlan_2*

次に、PBF_MAP_ACL を指定する例を示します。

```
Console> (enable) set pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 22
Commit operation successful.
Commit operation successful.

ACL 'PBF_MAP_ACL_11' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_11 successfully mapped to VLAN 11.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully committed.
Console> (enable)
ACL PBF_MAP_ACL_22 successfully mapped to VLAN 22.
Console> (enable) Operation successful.
Console> (enable)
```

PBF_MAP_ACL 情報の表示

PBF_MAP_ACL 情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF_MAP_ACL 情報を表示します。	**show pbf-map** {*vlan* | **config**}

次に、指定された VLAN の PBF 関連 ACE と、使用された各隣接の統計情報を表示する例を示します。

```
Console> (enable) show pbf-map 11
Index    DstVlan   DstMac             SrcMac          HitCount(hex)  Name
-----------------------------------------------------------------------------
1         22      00-00-00-00-00-02  00-00-00-00-00-00  0x00000000 PBF_MAP_ADJ_1
Console> (enable)
```

次に、PBF マップ設定の例を示します。

```
Console> (enable) show pbf-map config
set pbf_map 1.1.1.1 00-00-00-00-00-01 11 2.2.2.2 00-00-00-00-00-02 22
Console> (enable)
```

PBF_MAP_ACL 設定の消去

PBF_MAP_ACL 設定を消去するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF_MAP_ACL 設定を消去します。	**clear pbf-map all** | **vlan** *vlan* | *ip_addr_1 mac_1 vlan_1 ip_addr_2 mac_2 vlan_2*

次に、**set pbf-map** コマンドによって作成されたすべての ACL と隣接情報を消去する例を示します。

```
Console> (enable) clear pbf-map all

ACL 'PBF_MAP_ACL_11' successfully deleted.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully deleted.
Console> (enable)
```

次に、PBF_MAP_ACL_VLAN_# の名前を持つ ACL とその ACL が使用する隣接テーブルを消去する例を示します。

```
Console> (enable) clear pbf-map vlan 11

ACL 'PBF_MAP_ACL_11' successfully deleted.
Console> (enable) Commit operation successful.
Console> (enable)
```

次に、**permit ip any any** ACE を除いて **set pbf-map** コマンドによって作成された ACE をすべて消去する例を示します。コマンドによって、*vlan_1* および *vlan_2* 上の *ip_addr_1* および *ip_addr_2* であるホスト間のトラフィックをイネーブルにするエントリが削除されます。**clear security acl** コマンドによりエントリが削除済みの場合は、メッセージが表示され、特定のエントリが消去済みであることを示します。実際の削除されたエントリは、2 つの ACE（リダイレクト / 隣接 ACE）と、隣接テーブルの 2 つのエントリです。

```
Console> (enable) clear pbf-map 1.1.1.1 0-0-0-0-0-1 11 2.2.2.2 0-0-0-0-0-2 22

ACL 'PBF_MAP_ACL_11' successfully committed.
Console> (enable)
ACL 'PBF_MAP_ACL_22' successfully committed.
Console> (enable)
```

PBF 設定の拡張機能（Releases 8.3(1) 以降のソフトウェア リリース）

ここでは、Release 8.3(1) 以降のソフトウェア リリースで使用可能な 2 つのコンフィギュレーション コマンド（**set pbf client** および **set pbf gw**）を使用して PBF を設定する例を示します。ここで説明されている PBF 拡張機能は、セキュリティ ACL および隣接情報の設定とコミットのプロセスを簡略化します。拡張された **set pbf-map** コマンドは、入力に基づいてセキュリティ ACL および隣接情報を作成し、それをハードウェアにコミットして、VLAN にマッピングします。ある VLAN から別の VLAN へトラフィックをリダイレクトするために必要な VACL を作成する一部として、ARP パケットがソフトウェアにリダイレクトされてスーパバイザ エンジンがゲートウェイおよびクライアント要求に対する ARP 応答を生成します。

ここでは、PBF 設定の拡張機能について説明します。

- PBF の使用上の注意事項および制限事項（p.15-109）
- セキュリティ ACL および隣接情報の設定とコミット（p.15-109）
- clear コマンド（p.15-111）
- show コマンド（p.15-112）

- 診断インターフェイスとしての sc1 インターフェイスの使用（p.15-113）

PBF の使用上の注意事項および制限事項

ここでは、PBF を設定する際の使用上の注意事項と制限事項を説明します。

- Supervisor Engine 720 では、**set pbf vlan** *vlan* コマンドを入力して、PBF をイネーブルにしている VLAN を指定する必要があります。詳細については、「VLAN における PBF MAC アドレスの指定」（p.15-97）を参照してください。
- クライアントおよびゲートウェイは別の VLAN 上にあり、どのクライアントまたはゲートウェイにも同じ IP アドレスがないようにしなければなりません。エントリの最大数は 1024 です。
- クライアント名とゲートウェイ名は、12 文字以内でなければなりません。
- すでに VACL が添付されている 2 つの VLAN 間に PBF マップを作成する場合、PBF ACL が前の設定を上書きします。逆も成り立ちます。**set pbf-map** コマンドを入力して PBF ACL を作成し、PBF ACL が VLAN に添付されている場合、同じ VLAN に新しい VACL をマッピングしようとすると、新しい VACL が前の設定を上書きします。

セキュリティ ACL および隣接情報の設定とコミット

新しい **set pbf client** コマンドは、新しいホストに現在のリストを追加します。VLAN 接続を処理するゲートウェイを追加するのに新しい **set pbf gw** コマンドが使用されます。拡張された **set pbf-map** コマンドは、新しい 2 つの ACL（client_name および gateway_name）を作成し、新しく作成されたエントリをハードウェアにコミットし、それを VLAN にマッピングします。

PBF マップを作成するには、次の手順を実行します。

ステップ 1　次のように、各リストにクライアントおよびゲートウェイを追加します。

a. **set pbf client** *client_name ip_addr mac_addr vlan*

b. **set pbf gw** *gateway_name ip_addr ip_mask mac_addr vlan*

ステップ 2　次のように、クライアント リストをゲートウェイ リストにマッピングします。

set pbf-map *client_name gateway_name*

（注）　単一の PBF ゲートウェイにマッピングできる PBF クライアント グループの数は、すでに設定された ACL の数に依存します。サポートされている最大 ACL 数が 250 なので、すでに 20 ACL を定義している場合、229 のクライアント グループをゲートウェイにマッピングできます。

次に例を示します。

```
Console> (enable) set pbf client cl1 21.1.1.1 00-00-00-00-40-01 101
Commit operation successful.
Console> (enable) set pbf gw gw1 21.0.0.128 255.0.0.0 00-a0-c9-81-e1-13 102
Commit operation successful.
Console> (enable) set pbf-map cl1 gw1
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
.ccl1 editbuffer modified. Use 'commit' command to apply changes.
.ggw1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) ACL commit in progress.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully committed.
Console> (enable)
ACL '.ggw1' successfully committed.
Console> (enable) Mapping in progress.
Please configure VLAN 101.

ACL .ccl1 successfully mapped to VLAN 101.
Console> (enable) Mapping in progress.
Please configure VLAN 102.

ACL .ggw1 successfully mapped to VLAN 102.
Console> (enable)
```

新しく拡張されたコマンド セットは、次のコマンドの*すべて*と同等です。

```
#adj set
set security acl adjacency .c0001cl1 101 00-00-00-00-40-01 21.1.1.1
set security acl adjacency .g0002gw1 102 00-a0-c9-81-e1-13 21.0.0.128 7
#.ccl1
set security acl ip .ccl1 permit arp
set security acl ip .ccl1 permit arp-inspection any any
set security acl ip .ccl1 redirect .g0002gw1 ip host 21.1.1.1 any
set security acl ip .ccl1 permit ip any any
#.ggw1
set security acl ip .ggw1 permit arp
set security acl ip .ggw1 permit arp-inspection any any
set security acl ip .ggw1 redirect .c0001cl1 ip any host 21.1.1.1
set security acl ip .ggw1 permit ip any any
#
commit security acl all
set security acl map .ccl1 101
set security acl map .ggw1 102
```

set pbf-map コマンドによって追加された ACL 内の各エントリは、デフォルトの **permit ip any any** ACE の前に挿入されます。隣接にリダイレクトされる以外のエントリを追加する場合、**set security acl ip client_name** または **gateway_name** コマンドを入力します。ARP 検査エントリは、より個別なものに置き換えることができます。ARP 応答は、ARP 検査 ACE が確認されたあとにのみ生成されます。ARP 応答を取得できるクライアントを制限したい場合、新しい ARP 検査エントリを設定する必要があります。

clear コマンド

clear pbf client コマンドは、最初に PBF マップを削除せずに最後に残っている PBF クライアントを削除するのに使用できません。単一のクライアントまたはすべてのクライアントをリストから削除するには、ユーザ モードで次の作業を行います。

作業	コマンド
単一またはすべてのクライアントを消去できます。	**clear pbf** {**client** | **gw**} *name* [*ip_addr*]

次に、PBF クライアントを消去する例を示します。

```
Console> (enable) clear pbf client cl1
.c0001cl1 editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) Commit operation successfull.
Console> (enable)
```

clear pbf gw コマンドは、最初に PBF マップを削除せずに最後に残っている PBF ゲートウェイを削除するのに使用できません。単一ゲートウェイまたはすべてのゲートウェイを消去するには、ユーザ モードで次の作業を行います。

作業	コマンド
単一またはすべてのゲートウェイを消去できます。	**clear pbf** {**client** | **gw**} *name* [*ip_addr*]

次に、PBF ゲートウェイを消去する例を示します。

```
Console> (enable) clear pbf gw gw1
.g0002gw1 editbuffer modified. Use 'commit' command to apply changes.
Commit operation successfull.
Console> (enable)
```

PBF マッピングを消去するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF マッピングを消去します。	**clear pbf-map** *client_name gw_name*

次に、PBF マッピングを消去する例を示します。

```
Console> (enable) clear pbf-map cl1 gw1
.ccl1 editbuffer modified. Use 'commit' command to save changes.
.ggw1 editbuffer modified. Use 'commit' command to save changes.
Console> (enable) ACL commit in progress.
Console> (enable) ACL commit in progress.

ACL '.ccl1' successfully deleted.
Console> (enable)
ACL '.ggw1' successfully deleted.
Console> (enable)
```

show コマンド

PBF マップをすべて表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
すべての PBF マップを表示します。	**show pbf-map**

次に、すべての PBF エントリを表示する例を示します。

```
Console> (enable) show pbf-map
PBF MAP
Clients             Gatways
--------------------------------------------
cl1                   gw1
Console> (enable)
```

PBF クライアント設定を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF クライアント設定を表示します。	**show pbf client** [*client_name* | *ip_addr*]

次に、PBF クライアント設定を表示する例を示します。

```
Console> (enable) show pbf client
Client    : cl1
Map       : gw1
VLAN      : 101
Adjacency          ip           mac
----------------------------------------
.c0001cl1          21.1.1.1     00-00-00-00-40-01


Console> (enable)
```

PBF ゲートウェイ設定を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
PBF ゲートウェイ設定を表示します。	**show pbf gw** [*gw_name* | *ip_addr*]

次に、PBF ゲートウェイ設定を表示する例を示します。

```
Console> (enable) show pbf gw
Client    : gw1
Map       : cl1
VLAN      : 102
Adjacency          ip           mask           mac
----------------------------------------------------------------
.g0002gw1          21.0.0.128   255.0.0.0    00-a0-c9-81-e1-13


Console> (enable)
```

診断インターフェイスとしての sc1 インターフェイスの使用

使用しているスイッチと顧客のスイッチやルータとの接続テストを行いやすくするために、一時的に sc1 インターフェイスを PBF クライアント VLAN 内に配置する手順は、次のとおりです。

ステップ 1　**clear pbf arp-inspection** *list_name* コマンドを入力して、テストを行う ARP 検査 ACL ステートメントを PBF クライアント VLAN から削除します。

ARP 検査 ACE がクライアント リストまたはゲートウェイの ACL に設定されている（または設定されていない）ことを確認するには、**show pbf arp-inspection** コマンドを入力します。

ステップ 2　**set interface sc1** コマンドを入力して、sc1 インターフェイスを顧客の VLAN に割り当てて、それを顧客のルータまたはスイッチと同じ IP サブネットの IP アドレスに割り当てます。

ステップ 3　**ping** コマンドを入力して、（インターフェイス sc1 が送信元の）Catalyst 6500 シリーズ スイッチと顧客のルータまたはスイッチとの間で接続性をテストします。sc1 インターフェイスが顧客の MAC アドレスの ARP 要求を送信し、顧客のルータまたはスイッチが応答します。ICMP 応答が送信される前に顧客の装置が ARP 応答を送信した場合、sc1 インターフェイスは MAC アドレスで応答します。

ステップ 4　テストが完了したら、sc1 インターフェイスが顧客の VLAN の一部のままにならないように設定しなおします。

ステップ 5　**set pbf arp-inspection** *list_name* コマンドを入力して ARP 検査 ACL ステートメントを PBF クライアント VLAN に復元します。